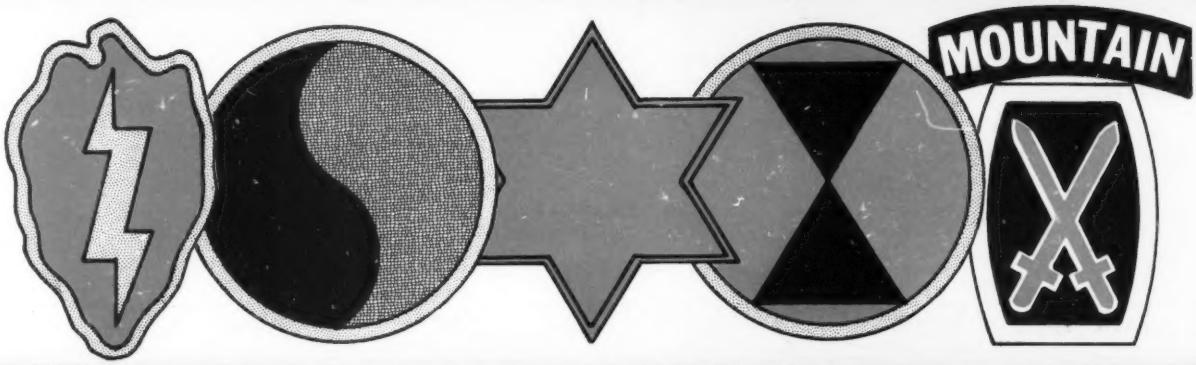
April-June 1985

Military Intelligence



LIGHT INFANTRY DIVISIONS

Features

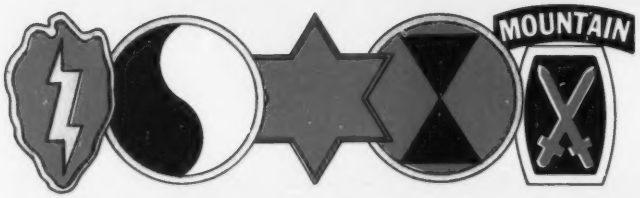
Military Intelligence is an authorized publication of the U.S. Army Intelligence Center and School, Fort Huachuca, Arizona, published quarterly under provisions of Chapter 5, AR 310-1. Unless specifically stated, material appearing herein does not necessarily reflect official policy, thinking or endorsement by any agency of the U.S. Army. Use of funds for printing this publication was approved by Headquarters, Department of the Army, December 1975. Use of the third person pronoun "he" and any of its forms, as used in this publication, is intended to include both masculine and feminine genders. ***Correspondence*** with ***Military Intelligence*** is authorized and encouraged. Inquiries, letters

Military Intelligence

From the Home of Intelligence

Volume 11 Number 2 April-June 1985

Departments



25th Infantry Division (Light)
29th Infantry Division (Light) NG
6th Infantry Division (Light)
7th Infantry Division (Light)
10th Mountain Division (Light Infantry)

Staff

Editor: *1st Lt. Stephen P. Aubin*
Assistant Editor: *Annette J. Castro*
Departments Editor: *Sp5 Robert A. Kerr*
Art Director: *Virginia C. Harris*
Illustrator: *Sp4 Donald L. Nelson*
Plans and Administration: *Sp5 Bernard L. Jamison*
Typographer: *Sp4 Warren J. Ford Jr.*

to the editor, manuscripts, photographs, and general correspondence should be sent to Editor, ***Military Intelligence*** Magazine, U.S. Army Intelligence Center and School, Fort Huachuca, Arizona 85613-7000. Telephone Autovon 879-2676/3266, commercial (602) 538-2676/3266. ***Subscriptions*** to ***Military Intelligence*** are available through the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
Controlled Circulation postage paid at Washington, D.C. **ISSN 0026-4028**

Cover Design
by Virginia C. Harris

from the Commander

by Maj. Gen. Sidney T. Weinstein

Intelligence support to the Light Infantry Division is an integral part of battle management. Given the austere nature and limited resources of the Light Division, intelligence support is absolutely essential to the successful planning and execution of the mission these divisions must accomplish. Our Military Intelligence Soldiers must not only be highly proficient in their MOS, but must possess the mental toughness and physical readiness required for success.

To this end, we recognize training requirements which will enable MI Soldiers to collect, process and disseminate intelligence useful to the unique requirements of the Light Infantry Division. Individual and team skills must be developed and evaluated by very rigid standards. Such tactical competencies include those required for maneuver unit planning, tactical movement of MI teams to isolated operational sites, and associated infantry skills.

Intelligence support to the Light Infantry Division will be provided by a 295-Soldier Military Intelligence Battalion. This battalion, recently approved by Department of the Army, has three organic companies: a Headquarters and Headquarters Service Company of 101 Soldiers; a Collection Company with 100 Soldiers; and an Intelligence and Surveillance Company of 94 Soldiers. Significant equipment will include three AN/TRQ-32 and nine AN/TRQ-30 radio receiving sets and 12 AN/PPS-15 ground surveillance radars. The battalion has no ground-based jamming capability because of personnel space constraints and sortie limitations. The total figure of 295 does not include the flight platoon. The flight platoon, consisting of 20 personnel and three QUICKFIX platforms, is organic to the Reconnaissance Squadron of the Combat Aviation Brigade. However, the MI Battalion will continue to exercise operational control over the flight platoon.

The Army will organize one National Guard and four active component Light Infantry Divisions. The 7th Infantry Division, Fort Ord, Calif., is currently scheduled to complete its conversion to a light configuration September 30, 1985. The 25th Infantry Division in Hawaii will begin its conversion in fiscal year 1986.

Other divisions which will convert to light infantry structure are the recently activated 10th Mountain Division (Light Infantry) at Fort Drum, N.Y., and the yet to be activated 6th Infantry Division in Alaska. The 29th Infantry Division, National Guard, has its headquarters at Fort Belvoir, Va.

The formation of these Light Infantry Divisions offers great challenges and opportunities for Military Intelligence. More now than ever before, our Soldiers must be tactically and technically competent so they can effectively support these forces in recognition of a continuing need for an immediate, credible, deterrent capability in an increasingly violent world. I am confident we will meet the challenge.

HOME OF MILITARY INTELLIGENCE

DUE TO A LACK OF PHOTOGRAPHIC CONTRAST BETWEEN TEXT AND BACKGROUND, THIS PAGE DID NOT REPRODUCE.

from the CSM

by CSM Robert H. Retter

Since 1982 we have been in the process of restructuring the three career management fields in Military Intelligence. To date we have implemented the restructure in one CMF, had one proposal returned for re-examination due to the Army of Excellence, and put one on hold for a year to validate training. I will address each CMF and bring you up to date on the current CMF status. Even though some of these restructuring changes have been published before, I believe it is important to keep you advised on all the CMF initiatives.

CMF 33

In December 1984 CMF 33 personnel from Fort Devens and MILPERCEN assigned soldiers in MOS 33S to one of five new MOS, two tactical and three strategic. The tactical MOS are 33R (EW/Intercept Aviation System Repairer) and 33T (EW/Intercept Tactical Equipment Repairer). The three strategic MOS are 33M (EW/Intercept Command and Central Repairer), 33P (EW/Intercept Receiving Systems Repairer), and 33Q (EW/Intercept Processing and Storage Equipment Repairer). The restructure of CMF 33 took place in March 1985.

Another change that will occur for CMF 33 is the addition of the MOS 33V in FY 87. On February 8, 1985, the Deputy Chief of Staff for Personnel approved the transfer of Proponency for MOS 26E and 26F from the U.S. Army Signal Center at Fort Gordon to the U.S. Army Intelligence Center and School. The two MOS will merge into CMF 33 and will eventually be redesignated as MOS 33V. Upon implementation of MOS 33V, all initial entry personnel will be required to have a Top Secret clearance and be eligible for Special Intelligence access. Personnel currently holding MOS 26E or 26F must submit for a Top Secret based on a Special Background Investigation. 33V soldiers will become 33R at grade E7 and will cap at 33Z. 26F will become an additional skill identifier for 33V. Soldiers holding MOS 26E or 26F will attend the Advanced Noncommissioned Officer Course for CMF 33. Attendance requires a TS/SI clearance.

CMF 96

CMF 96 was returned in April 1985 for re-examination due to the Army of Excellence. We have had some non-structural changes approved.

MOS 17K and 17M were combined into MOS 96R. Implementation began in March 1985. MOS 17M is now an ASI for 96R and personnel going to the 82nd Airborne Division will receive remote sensor training after completing ground surveillance radar training. All initial entry personnel will be required to have a Secret clearance.

As of March 1985 MOS 96C became 97E and was moved from subgroup 96 to subgroup 97. Also personnel going into MOS 97E will now receive language training at the Defense Language Institute prior to MOS training.

The reinstated 97B10 program is an extremely valuable method of correcting the current grade infeasibility of MOS 97B, resolving the chronic shortage and providing a more experienced and capable 97B20. I addressed the program in my last column and more information is outlined in the "Enlisted Notes" in this issue.

MOS 96H was to progress from grade E1 to E8 under the original restructure. Because of the low density of the MOS we could not justify E8 positions. The 96H will continue to feed MOS 96D at E8. Once J-STARS is fielded, the number of 96H will increase and be able to support a number of E8 positions.

CMF 98

Restructure of CMF 98 was put on hold for one year to validate the collection/analysis training. The only nonstructural change is moving MOS 05G from CMF 98 to CMF 96 and making it MOS 97G. This was implemented March 1, 1985.

The restructuring of the Military Intelligence career management fields is progressing at a satisfactory rate. The result will be better career progression, less crossover from one MOS to another, and improved advancement potential. I will keep you informed of the changes as they are approved.

LEAD BY EXAMPLE

DUE TO A LACK OF PHOTOGRAPHIC CONTRAST BETWEEN TEXT AND BACKGROUND, THIS PAGE DID NOT REPRODUCE.

Behind the Lines

This column is introduced in ***Military Intelligence*** as a forum which the editor will use to articulate certain ideas relating to the Magazine's features or its overall direction. In this column, the editor will attempt to synthesize ideas, raise issues, and provoke responses.

Military Intelligence is our Branch professional journal. As such, it provides an important forum for the discussion of ideas within the MI community. The quality of the Magazine depends on the willingness of people at all levels throughout the intelligence community to contribute. But to just contribute "what the Center and School" or "what senior officers" want to hear falls far short of what is required in a *forum*. A forum is only created through dialogue. In this case, true dialogue must occur between the Intelligence School (trainers, training developers, doctrine writers, and combat developers) and the field (those who put policy into practice).

In the tactical environment, there are instances where, rather than responding with constructive criticism and suggestions for improving a doctrinal position, a unit will just disregard the tenets and do what works at the time. Doctrine embodies fundamental principles by which our military forces guide their actions. While the fundamental principles enjoy a certain longevity, the tactics, techniques, and procedures, or the "how" of doctrine, must respond to METT-T and change as field units refine them through application. Improvements in the tactics, techniques, and procedures associated with doctrine can only occur if field units provide the necessary feedback. Besides the continual interaction which must occur between the field and the doctrine writers, our Branch journal can help bring doctrinal issues of importance to the attention of the intelligence community at large.

Our Branch journal must reflect the proper balance between doctrine and practice. We encourage all intelligence personnel to consider making a contribution. The editorial staff will review all submissions for publication and respond to authors as to its decisions. The editor should be a facilitator, one who ensures that diverse viewpoints are expressed. However, before an editor can do this job, the Magazine must have something to work with. We are here to serve the entire intelligence community. All ideas are welcome. Remember, by not expressing your idea, you may be depriving the intelligence community of a great opportunity.

The Editor

FEEDBACK

Editor:

It is with some distress that I read 1st Lt. Christopher Hennen's article, "Terrorism in Northern Ireland" in the October-December issue. Though the author never expressly recommended adopting British counterterrorist tactics, this was, to a great extent, implied.

The British role in Northern Ireland is a counterinsurgency model which we should diligently avoid. Hennen states, "Because of the unremitting efforts of the British security forces, terrorism has failed to gain a firm hold over the population." The evidence since 1969 suggests, however, exactly the opposite. Many observers would say that the "unremitting efforts of the British security forces" are precisely what has enabled the IRA to gain the support of large segments of the population. (In recent elections SINN FEIN, a legal pro-IRA political party, received over 100,000 votes across Ulster.) The author effectively provides the reasons for this apparent paradox in the text of his article.

In the six counties of Northern Ireland, the British have adopted draconian security measures unique among Western nations. Many of these actions are clearly inimical to American concepts of "due process" and civil rights. It is essential to remember that these measures are being conducted against a group of people Britain considers its own citizens. The Emergency Provisions Act mentioned by Hennen, along with the Prevention of Terrorism Act, deprived arrested suspects of the right to silence and enabled the arresting agency to hold a suspect without charge, incommunicado, for up to seven days. After charged, a suspect could remain in custody for up to two years awaiting trial. The author describes the "P-tests" whereby suspects are selected at random and required to provide information on "families, friends, occupation and religious affiliations and involvements." In 1975, the British were able to claim that nearly 40 percent of the Ulster population had been fed into its computer. (Interestingly, nearly 40 percent of Ulster's population is Catholic.)

The article continues the litany. Terms such as "covert photographic surveillance," "internment," "sensory deprivation" and "deep interrogation" should not and do not inspire enthusiasm among citizens of a democratic country. Plainclothes members of the "world's finest anti-terrorist commando unit," the SAS, have been detained and disarmed in the Irish Republic by Irish police officers after the SAS team became "lost."

The IRA was a ludicrous anachronism in Ulster before 1969. Since the British countermeasures were widely employed, the alienation of one third of the province's population has escalated alarmingly. The way forward in Northern Ireland requires infinitely more than a "police force" with a "well-regulated intelligence capability."

After our own HUMINT collection problems in CONUS in the late 1960s and early 1970s, MI personnel, above all should rigidly avoid creating the impression that we admire counterterrorism as practiced in Northern Ireland.

Capt. Thomas J. Howley
Co. A, 302nd MI Battalion
Frankfurt, West Germany

Editor:

For those of us on the "front line of terrorism," your October-December 1984 edition, "Terrorism Counteraction," was timely, to-the-point, and extremely useful. We who serve here in South and Central America experience the threat, frequently first-hand, and need any and all the expertise we can get. I, for one, am very pleased that USAICS is taking the lead in this vitally important area, one which for us attaches can mean our very survival. USAICS' initiative in teaching terrorism-counterterrorism to several officer and specialty courses can truly serve as an example to the other services that the U.S. Army is aware of and prepared to fight this threat to world stability. Please pass on to the Commander, to the ***Military Intelligence*** *staff and to the authors my thanks and congratulations for a fine series.*

Lt. Col. David R. Stevely
Assistant Army Attache
U.S. Embassy, Caracas, Venezuela

Editor:

I am very pleased that my comments in the April-June 1984 issue have generated some reaction. At least this means people are thinking about the problem and not just running on inertia.

In response to CW3 (George F.) O'Connor: Thank you. This is exactly the "politics" I was talking about. MI units should be crammed down the throats of the adjutants general by DA and the National Guard Bureau. By adding MI companies and battalions to National Guard division and separate brigade tables of organization, the assertion that they are useless may not arise. Artillery has no stated mission either—as such.

O'Connor's observation on MI unit location does not seem to track with what we see in the Southeast. Areas with high densities of electronic and linguist talent (e.g., the Research Triangle in North Carolina, Greenville-Spartanburg in South Carolina) are not exploited. Neither is the vast array of talent leaving Fort Bragg's myriad MI units and remaining in North Carolina.

The policies cited by O'Connor are important. But other policies should influence "intelligence organization and stationing" in the Reserve component as well: Unity of command; esprit de corps; combined arms coordination.

The following description of a separate brigade and its MI support is based on shallow observation of several such relationships in the Southeast; any resemblance to a real unit is purely coincidental:

- *The brigade has a CAPSTONE mission from AFCENT, but its supporting ASA and MI units have Russian linguists (if any).*
- *The supporting units, soon to become one company, are at three separate locations in three states, all at least 300 miles from each other and the supported brigade's headquarters.*
- *The brigade and its supporting ASA and MI units are issued four different CEOI by their respective higher headquarters.*
- *Nobody in the entire brigade has SCI access.*
- *The brigade has never had a brigade or battalion S2 who has attended MIOAC or even MIOBC (resident or nonresident).*
- *The ASA company has its Annual Active Duty Training with the brigade about every other year; the other detachments go with the brigade even less often.*
- *Brigade and MI/ASA unit personnel never see each other on weekend drills.*

This picture should not be taken as a criticism of any particular individuals. All of those involved have many other things on their minds; the system is not set up to facilitate pre-M Day coordination. How will this brigade survive when deployed?

There are problems with assigning MI units to the National Guard; there are costs. But the potential cost of not doing so is much, much higher.

*In response to Mr. (Michael) Evancevich: there is finally a good, exciting novel starring an analyst—**The Hunt for Red October** by Tom Clancy, published by Naval Institute Press at Annapolis.*

Capt. Edward M. McClure
139th Rear Area Operations Center
North Carolina Army National Guard

Editor:

*Col. (Basil J.) Hobar's article (October-December 1984) on the intelligence effort during the German Ardennes offensive of December 1944 is extremely interesting, especially when contrasted with "Armor's Last Stand at St. Vith," (**Armor** November-December 1984) and the conclusions drawn by the author, Capt. Stephen D. Burrows, on the Allied intelligence performance in the campaign. The effectiveness of German deception is certainly an object lesson appropriate for AirLand warfare today.*

Another point of interest in the study of the Ardennes fight concerns a more subtle, but very human and little known factor. Lt. Gen. (Courtney H.) Hodges, then Commander, First U.S. Army, relieved his G2 in late November because of that officer's insistence that the Germans were, in fact, in an offensive build-up posture. Small wonder that his replacement and the VIII Corps G2 lowered the counterattack capability in the order of priority. This, taken with the fact the Allied Airborne Army Intelligence Officer was also relieved just before Market Garden the previous September (for steadfastly sticking to the notion that the Germans had armor in the British objective area), must have made for an interesting professional climate for intelligence officers that fall and winter.

Our business certainly has its occupational hazards. I believe that the climate has vastly improved, but we still need to be prepared to risk all and stand by our guns when the facts support it. Anything less could result in as many lost lives as were suffered in December 1944 and January 1945, and then perhaps worse.

Lt. Col. Wayne E. Long
Commander, 108th MI Battalion
8th Infantry Division (Mechanized)

Editor:

Along with the tactical and technical skills every officer must possess, far and away the key to preparation for officership is a set of ethical values upon which the officer corps was founded and which is, or should be, the cornerstone of the corps. Despite varying levels of proficiency, based on schooling and training, a new lieutenant has to have an unwavering mindset that the driving force in all decision making is simply to do what's right.

Only through a sincere and dedicated effort in doing what's right all the time *can an officer gain the trust of his superiors, peers, and by far most importantly, his subordinates. A willingness to sacrifice and a genuine caring are complementary ingredients of this formula.*

I contend that all service schools train each lieutenant in the tactical and technical skills to at least a satisfactory level of competency. This knowledge can be honed and refined upon initial assignment. However, integrity must be internalized—no room for compromise, honing or refinement—it is essential and must exist upon assignment. From the first decision to the last, the officer has to base each decision on the overall welfare of his people and the organization. One has to weigh these two factors and not necessarily the whims of his superiors. He must be prepared to say "no," if appropriate, and present viable alternatives to the situation. The officer can never stray from this ethical base because when the time comes to "lay the bar on the line," that ethical base is the only credibility one will have to fall back on. Any previous breaches of integrity will surely crumble that base.

The trust which is bestowed with our commission has as its mainstay integrity above all. We are entrusted with the safety of our nation and her people, but we are above all charged with the responsibility of representing all those ideals our country stands for. Those ideals are that which set us apart and above all other nations. The key to officership is an uncompromising clinging to these values and ideals, with a confidence that adherence to them will overcome any and all adversity.

1st Lt. Mark J. Lansing
Department of Surveillance and
Systems Maintenance, USAICS
Fort Huachuca, Ariz.

Editor:

*There are two small related errors in the Crossword and Cryptocorner features of the October-December 1984 issue of **Military Intelligence**. Answer 5 Down of the Crossword should be Hindenburg, not Hindenberg. The 1914 Russian disaster was the Battle of Tannenberg, not Tannenburg. Burg, in German, means "fortress," Berg is mountain. In German, they are also pronounced differently. Hindenburg was the victor at Tannenberg.*

In 1410, near Tannenberg, Polish forces under Wladyslaw Jagiello defeated the Teutonic Knights, in a battle usually known as Grunwald.

*Cryptocorner and the Crossword Puzzle are only two of the excellent features of **Military Intelligence**. We have received **Military Intelligence** since November 1981, Volume 7, Number 4. Is it possible to obtain back issues prior to that number?*

Erhard F. Konerding
Documents Librarian
Wesleyan University
Middleton, Conn.

Mr. Konerding:
*No back issues of **Military Intelligence** are available. Requests for photocopies of specific articles or microfiche copies are considered on a case-by-case basis.*

The Editor

Military Intelligence

Order Form Mail To: Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

Enclosed is $ _____ ☐ check, ☐ money order, or charge to my Deposit Account No.

☐☐☐☐☐☐☐–☐

Order No._____

MasterCard and VISA accepted.

Credit Card Orders Only
Total charges $_____
Fill in the boxes below.
Credit Card No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
Expiration Date Month/Year ☐☐☐☐

Customer's Telephone No.'s
Area Code | Home | Area Code | Office

Charge orders may be telephoned to the GPO order desk at (202)783-3238 from 8:00 a.m. to 4:00 p.m. eastern time, Monday-Friday (except holidays).

Please enter my subscription to MILITARY INTELLIGENCE *[MILIN] for one year at $14.00 Domestic; $17.50 Foreign.*

Company or Personal Name
Additional address/attention line
Street address
City State ZIP Code
(or Country)

PLEASE PRINT OR TYPE

For Office Use Only

Quantity	Charges
_____ Publications	
_____ Subscriptions	
Special Shipping Charges	
International Handling	
Special Charges	
OPNR	
_____ UPNS	
_____ Balance Due	
_____ Discount	
_____ Refund	

982

Military Intelligence

Order Form Mail To: Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

Enclosed is $ _____ ☐ check, ☐ money order, or charge to my Deposit Account No.

☐☐☐☐☐☐☐–☐

Order No._____

MasterCard and VISA accepted.

Credit Card Orders Only
Total charges $_____
Fill in the boxes below.
Credit Card No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
Expiration Date Month/Year ☐☐☐☐

Customer's Telephone No.'s
Area Code | Home | Area Code | Office

Charge orders may be telephoned to the GPO order desk at (202)783-3238 from 8:00 a.m. to 4:00 p.m. eastern time, Monday-Friday (except holidays).

Please enter my subscription to MILITARY INTELLIGENCE *[MILIN] for one year at $14.00 Domestic; $17.50 Foreign.*

Company or Personal Name
Additional address/attention line
Street address
City State ZIP Code
(or Country)

PLEASE PRINT OR TYPE

For Office Use Only

Quantity	Charges
_____ Publications	
_____ Subscriptions	
Special Shipping Charges	
International Handling	
Special Charges	
OPNR	
_____ UPNS	
_____ Balance Due	
_____ Discount	
_____ Refund	

982

Book Review Policy

Book reviews are considered to be an integral part of the presentation of information of professional interest to the MI community. The normal policy of ***Military Intelligence*** is to publish reviews of books which have appeared in print over the previous year. Book reviews which are more than one year old are only published in cases where useful subject matter might not otherwise have been brought to the attention of our readers. Such reviews are considered on a case-by-case basis. Reviews of current books are more likely to be published. A limited number of books are received directly from publishers and are available for review. If you are interested in reviewing one of these books, please contact the editorial staff. Unsolicited reviews are also welcome and encouraged.

"Feedback" is the readers' column, *your* column. Letters printed in "Feedback" can be on any subject that relates to intelligence, electronic warfare, doctrine, tactics, innovations from the field, suggestions, criticism, even praise, or anything else the readers of ***Military Intelligence*** may find of interest. Letters *do not* have to refer to a previously printed article or letter from the magazine to be used in

FEEDBACK.

Letter Policy: All letters to the editor must be signed. Names may be withheld if requested. Letters should be type-written and double spaced. The editor reserves the right to shorten letters. Letters are normally edited for style, grammar, spelling and punctuation. Please include a phone number (Autovon preferred) and a complete return address on the letter itself (envelopes tend to get separated from the letters).

Military Intelligence Writer's Guide

MILITARY INTELLIGENCE is oriented toward active Army, reserve and civilian intelligence personnel throughout the Army and Defense intelligence communities. When writing an article, consider the readers. They range from privates to general officers to civilians, and they all have one thing in common: they work in, or have interest in, military intelligence.

SUBJECTS: We are interested in all subjects relating to the diverse fields of military intelligence including Army doctrine and policies relating to intelligence; tactical and strategic intelligence; organization; weapons and equipment; foreign forces; electronic warfare; and intelligence collection (SIGINT, HUMINT, IMINT, ect.). Historical articles should have contemporary value. If you have an idea for an article, contact us and explain your theme, scope and organization. It will save both of us time and will facilitate our planning.

STYLE: **Military Intelligence** prefers concise and direct wording in the active voice. Every article should have a beginning that catches the readers' attention, a body containing the crux of the article, and an ending which concludes or summarizes. Keep the article as simple as possible. Avoid unfamiliar terms, unexplained abbreviations, and poorly constructed sentences. Don't submit a manuscript unless you are completely satisfied with it. Read it over three or four times and then let a friend read it. It is not uncommon to revise an article several times before submitting a finished manuscript. Don't waste the readers' time with meaningless or repetitive phrases or words. We edit all articles. However, a polished article is more likely to be accepted than a hurried mistake-riddled effort. Save yourself time and effort; be your own editor. We do not normally allow writers to review how their articles have been edited.

ACCEPTANCE: We make no prior commitments on acceptance until we have thoroughly studied each manuscript. All manuscripts must be original, previously unpublished works. Authors submitting articles are responsible for informing the staff of **Military Intelligence** of simultaneous submission and/or acceptance by other publications.

FORMAT: We prefer articles from 1,000 to 2,500 words in length. We will publish shorter or longer articles depending on quality. Develop your ideas and stop. Send clean, doublespaced manuscripts typed on one side of the sheet. Your name, length of manuscript, address, and phone number (Autovon preferred) should be typed on the first page. We prefer one original and one copy. Cite your references and enclose all quoted material in quotation marks. If possible, credit should be given within the article as footnotes are burdensome and use valuable space.

GRAPHICS: Artwork in the form of black and white glossy photographs, maps, sketches or line drawings can enhance the attractiveness and effectiveness of your article. If you have an idea for artwork or know where we can get it, let us know.

CLEARANCE: All service members and Department of Defense civilians must clear articles through their local security office prior to submission. A signed statement of clearance must accompany the article. Certain categories of articles, as outlined in AR 360-5, must be cleared through the Office, Chief of Public Affairs, Department of the Army. Your local information officer can assist with this.

BIOGRAPHY: Enclose a brief biographical sketch, including important positions and assignments, experience or education which establishes your knowledge of the subject, and your current position and title. Photos of authors are no longer used in **Military Intelligence.**

COPYRIGHT: **Military Intelligence** is not copyrighted. Acceptance by **Military Intelligence** conveys the right for subsequent reproduction and use of published material for training purposes.

If you are interested in a subject, chances are that others will be too. Pick a subject, thoroughly research it, and think all your ideas through. Write with enthusiasm, but be natural. Don't adopt a different style.

For more information, contact the editor by writing to Commander, USAICS, ATTN: ATSI-TD-MIM, Fort Huachuca, Ariz. 85613-7000; or call Autovon 879-2676/3266, or commercial (602) 538-2676/3266.

Evolution of the MI Battalion in the Army of Excellence

by Capt. Patricia A. Rust

During the past 18 months the Army has sustained a dynamic modernization process unsurpassed since World War II. Comments made by Army leaders during the 1983 Fall Commanders' Conference culminated in a new concept referred to as the Army of Excellence. Inadequate strategic airlift and personnel requirements far in excess of congressional authorizations compelled the Army to restructure the force. The U.S. Army Intelligence Center and School became an active participant in developing Military Intelligence organizations to support the Army of Excellence. The history and eventual results of these efforts are discussed here.

The catalyst for the restructure was the 1983 Fall Commanders' Conference at which MACOM commanders expressed their dissatisfaction with a system that could not provide authorized personnel or equipment. As a result Gen. John A. Wickham Jr. directed that the Army be redesigned, within congressional authorization. Manpower constraints and deployability considerations provided the impetus for evaluating the Division 86 Force structure. Various studies revealed that the U.S. Air Force did not have the capability to deploy division assets with the current C-141 fleet; however, Congress would not appropriate additional monies to increase airlift capability. Historically, emphasis had been placed on developing equipment for the NATO scenario which envisioned heavy combat forces opposing Warsaw Pact divisions. Unfortunately, strategic airlift capability did not increase proportionately with heavy equipment development. The Grenada intervention demonstrated the necessity for a highly mobile infantry division with the ability to respond rapidly to worldwide low intensity contingencies in minimal time.

Manpower constraints were additional aspects of the force structure requiring immediate attention. A programmed force capability analysis revealed that 300,000 more personnel were required to man the Division 86 Force than Congress was willing to finance. Wickham insisted this was untenable and that authorizations should be equivalent to requirements. The Deputy Chief of Staff for Operations was the broker for manpower

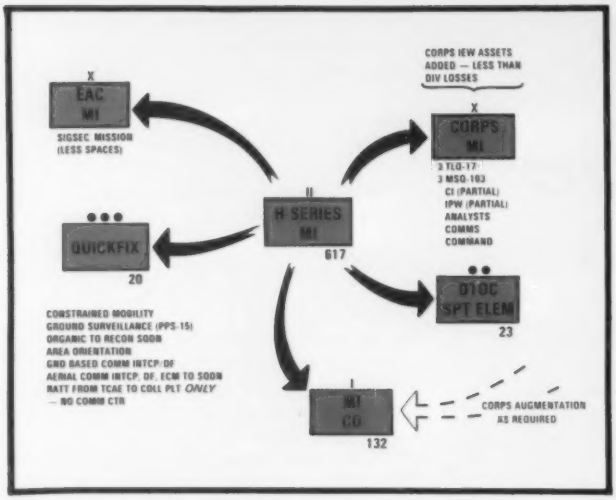


Figure 1

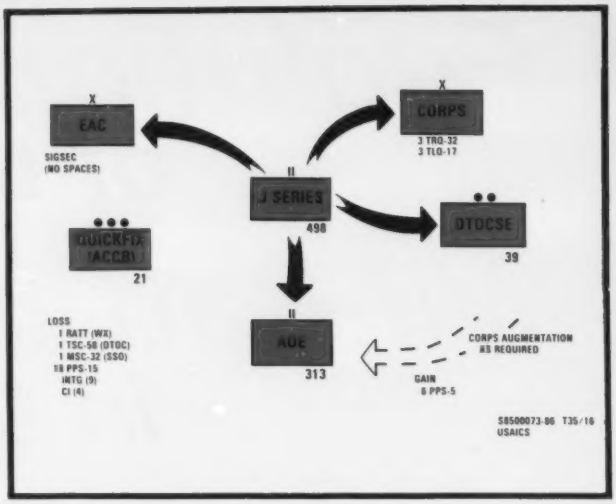


Figure 2

spaces and through a series of meetings held during the fall of 1983 determined the number of personnel for divisions, corps, and echelons above corps.

This initial effort resulted in a light division structure of approximately 10,000 personnel optimized for low intensity conflict: primarily, foot-mobile dismounted infantry with helicopter support; self sufficient for 48 hours; and deployed in less than 500 sorties. Two new light divisions were authorized; and in order to pay the manpower costs, heavy divisions and echelons above corps were reduced.

The original MI unit designed to support the infantry division was a 132-person company and was organic to the reconnaissance squadron of the combat aviation brigade. The division tactical operations center support element was reassigned to the headquarters and headquarters company of the division under the control of the division G2, while the technical control and analysis element remained organic to the company. QUICKFIX was retained in the division, but as an element of the headquarters and headquarters troop of the reconnaissance squadron. (See figure 1.) The decision to delete ground-based jammers and ELINT collection resulted from sortie constraints as well as the low intensity conflict orientation of the light division. To retain this capability for support to the division commander, these IEW assets were placed in the light corps, MI brigade, tactical exploitation battalion for augmentation to weight the battle, when required.

In addition to guidance provided for constructing a light infantry division, Wickham stated that a new heavy division would be organized and employed primarily for mid to high intensity conflicts and sustained combat operations in a European scenario. The heavy division was not constrained by strategic mobility requirements and, therefore, was provided the option of heavy equipment and vehicular mobility absent from the light division. However, a reduction in size was prescribed predicated on providing spaces for the new light division.

The MI battalion supporting the heavy division was reduced from the Division 86 Force of 498 to 313 personnel. (See figure 2.) While IEW capabilities were reduced, the organizational structure remained a battalion. Retained capabilities were those absolutely essential for intelligence collection, processing, dissemination, and electronic warfare. This included TACJAM, TRAILBLAZER and TEAMPACK, as well as counterintelligence and prisoner of war interrogation. To remain within congressional authorizations and provide heavy divisions with adequate IEW assets, the voice collection capability (AN/TRQ-32) was transferred to the heavy corps MI brigade to be used as augmentation to the division, if required. Paralleling the light division, the DTOCSE became organic to the headquarters and headquarters company of the division as a G2 asset, and the technical control and analysis element remained organic to the battalion.

Although these organizations were approved and scheduled to be implemented, several events led to a decision to request an increase in MI assets assigned to both light and heavy divisions. An Analysis of Military Organization Effectiveness study, completed in the summer of 1984, revealed that the MI company was too austere to perform its mission. Additionally, during the Army Commanders' Conference, held in August 1984, key field commanders indicated their support for an increased MI force structure. Another reason for the demise of the original concept was the concern that equipment habitually operating in the division area should be a divisional asset.

On October 2, 1984, Gen. William A. Richardson tasked the Intelligence School to re-evaluate the MI force structure and design a structure paralleling the airborne and air assault MI battalions. This process, referred to as "Relook," began to build a viable

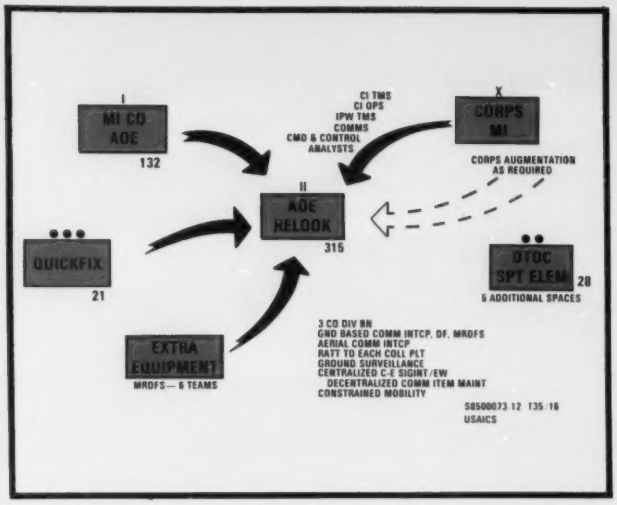


Figure 3

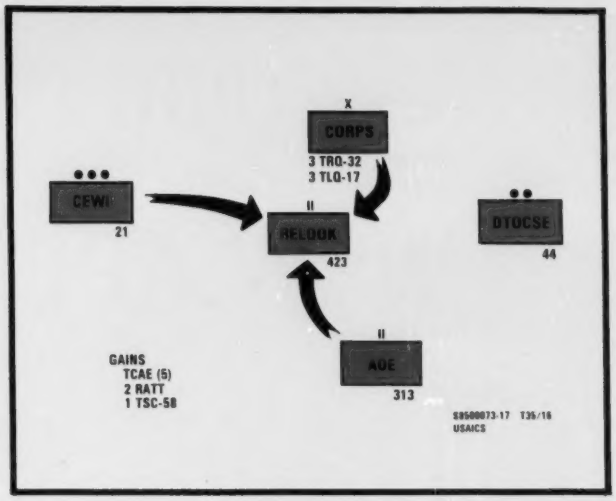


Figure 4

intelligence organization and establish priorities for the new structure. To provide the division commander with a responsive intelligence system, the first priority was to make the MI unit organic to the division and increase the organization to a battalion strength of 315. This move added the experience of a lieuteant colonel directing intelligence collection efforts. Additionally, concern for the low intensity conflict orientation of the battalion established the need to increase the counterintelligence and interrogation capabilities. Furthermore, the orientation toward a low intensity conflict increased demands for AN/PPS-15 ground surveillance radars, expanding the teams by six additional radars. Perhaps the most significant addition to "Relook" was the reintroduction of the QUICKFIX platoon into the MI battalion. QUICKFIX provides a flexible EW asset, critical in providing intelligence to the commander. (See figure 3.) Of course, the QUICKFIX issue has been challenged and it is very likely the aircraft will be returned to the aviation battalion.

During "Relook" at the divisional MI support structure, the heavy division was scrutinized for mission performance. Based on suggestions presented by Gen. Glen K. Otis, assets usually operating in the division area were placed back in the division, increasing personnel from 313 to 423. Assets returned to the battalion include the AN/TLQ-17, AN/TRQ-32, and QUICKFIX. (See figure 4.)

Although "Relook" did not restore all the assets organic to Division 86 Force MI organizations, the new structures provide flexibility, resiliency and the command and control necessary to conduct intelligence operations. "Relook" is a vast improvement over the original Army of Excellence design and reflects the Army's commitment to provide timely and accurate intelligence to the commander. ★

Capt. Patricia A. Rust is currently assigned as an action officer for the Directorate of Combat Developments, U.S. Army Intelligence Center and School, Fort Huachuca, Ariz. She has served as Executive Officer for the 226th AG Company (Postal), and Assistant S1 with the 66th MI Group, both in Munich, Germany. Rust graduated Magna Cum Laude from Sam Houston State University in 1974 earning a BA in European History. She earned her MA in International Relations in 1982 from the University of Southern California. Her military education includes the AG Officer Basic Course, the MI Officer Advanced Course and the EW/Crypto Officer Course.

Editor's Note: As this article was going to press, a decision was made by the Commanding General, TRADOC, to return QUICKFIX to the combat aviation brigade.

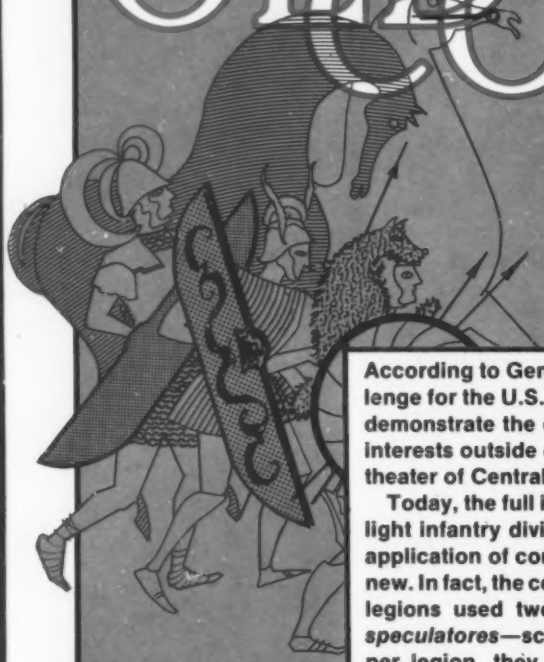
LIGHT INFANTRY

NEW APPLICATION

OF AN

OLD CONCEPT

by Maj. J. F. Holden-Rhodes



According to Gen. Edward C. Meyer, the most demanding challenge for the U.S. Army in the 1980s will be to " . . . develop and demonstrate the capability to successfully meet threats to vital interests outside of Europe, without compromising the decisive theater of Central Europe."[1]

Today, the full impact of that statement has come home as the light infantry division becomes reality. The LID represents the application of concepts that might, at first glance, appear to be new. In fact, the concept is as old as recorded history. The Roman legions used two types of light infantry. The first were the *speculatores*—scouts. Although there were only 10 *speculatores* per legion, they were an important component of the army. Within the legion they formed a reconnaissance squad and quite often the *speculatores* of each legion were grouped together for large scale reconnaissance missions.

The light infantry or *velites* of the legions were organized into *cohorts*, the equivalent of the present day battalion. The *velites* were deployed to the front and flanks of the legion battle formation. Behind them stood the *hastati* and the *principes*, the first and second lines of the legions' heavy infantry. The *velites* were trained so that, in addition to their other skills, they could operate in regular formations with the heavy infantry.

S. L. A. Marshall, in what many consider to be his most important work, **The Soldier's Load and the Mobility of the Nation**, wrote admiringly of the speed, skill and flexibility of the Roman soldier. Marshall emphasized that while the training of the legions was very important, it was their lightness of equipment that allowed them their speed and flexibility. Despite the fact that each man had to carry his armor at all times, as well as a 50-pound load of personal equipment and 15 days rations, the legions were still fleet of foot. Marshall went on to argue that it was most important not to overload the soldier, for, in so doing, his mission would be more and more difficult, if not impossible. The key to success was mobility, matched by weaponry that would enable the soldier to win on the battlefield. Clearly that goal is as important today as it was when the legions fought to hold on to the world of their day.

To understand the modern light infantry concept, one must look back to see why the application of light infantry forces has taken on such significance in politico-military affairs.

From the post-World War II period, the strategy of the United States and NATO was built around the employment of nuclear weapons. As Noel Parrish noted in his book, **Behind the Sheltering Bomb**, the United States viewed the harnessing of the atom and the nuclear weapons that were subsequently created as the reins by which any aggressor could be held in check. The essence of that strategy was the protection and defense of Fortress Europa. It was held that the sparks of the next war would be ignited in Central Europe. When the Soviet Union exploded its first nuclear weapon, total dependence upon nuclear deterrence went out the window.

Concurrent with the advent of the Atomic Age and the loss of U.S. strategic nuclear dominance, the concept of "wars of national liberation" was conceived and set into operation by the Soviet Union. It has been this mode of warfare by which the Soviet Bloc has made its most significant strides. Looking at this phenomenon today, it is clear that the Soviets, early on, opted for a multifaceted approach as they sought the realization of their goals. This fact is brought home now, as the United States continues to place increasing emphasis on low intensity conflict. This strategy obviously is a direct response to counter the seemingly ubiquitous wars of national liberation and other methods of Soviet expansion.

Since the early 1950s the Army has faced a challenge that was sometimes held to be mutually exclusive. The maintenance and support of the forces to defend Europe appeared at loggerheads with the increasing requirement to meet threats to the United States, outside of Europe. After 30 years of being in this dilemma, the concept and employment of the light infantry divison appears to be the sword to cut this Gordian knot. Of great significance is the fact that the employment of the light divisions can be a proactive rather than a reactive sword when it is wielded by the hand of intelligent foreign policy.

Citing the need for a flexible response force, current doctrine suggests that, "To improve the Army's capability to meet security demands within the dynamic and volatile international environment, a requirement exists for a strategically responsive and flexible infantry division. This division is organized, equipped and trained to respond to a broad spectrum of contingencies and to reinforce foward deployed forces. It focuses on defeating light enemy forces while retaining utility for employment in other scenarios."[2]

Retired Army Lt. Gen. James F. Hollingsworth put it even more succinctly: "The maneuver ground forces (light infantry) must be able to quickly concentrate at critical points and produce the necessary lethality. They are needed to ensure success in urban or forested areas. They are needed to screen and provide other capabilities traditionally performed by the cavalry. They are needed to deploy combat power to areas of the world where we cannot now bring that power to bear in sufficient amounts to be credible. They will be used tactically in much the same way a pack of hunting dogs attacks a wild boar—move, attack, evade, move and attack again, until their quarry is worn down and dispatched."[3]

The 25th Infantry Division in Hawaii, the 6th Infantry Division in Alaska, the 7th Infantry Division in California, the new 10th Mountain Division (Light Infantry) and the 29th Infantry Division all have been designated as light infantry divisions. The rationale behind the selection of the 29th, which is a National Guard unit, is that the Guard provides the Army with between 60 and 70 percent of its combat punch (within the total force structure).[4] It is of some interest to note that discussion is presently ongoing concerning the use of mules for the 10th Mountain Division (Light Infantry). (The 10th is the grandson of the 10th Mountain Division of World War II fame.)[5]

Formation of the new light divisions will not involve additional requests for funding, since they will be created using existing troops and resources. It has also been projected that there will be no significant change in the Army's overall end strength. The standard division has approximately 18,500 soldiers; the new light divisions will have about 10,700. When the "tooth to tail" ratio is compared, the former is found to have only 16 percent of its strength in fighting billets, while the latter will have one third of its soldiers as fighters.

The light division will be equipped with approximately 8,500 M16 rifles, 162 Dragons and 44 TOWs. A 99-helicopter combat aviation brigade includes attack, reconnaissance, and troop lift types.[6] Division artillery assets consist of three battalions equipped with 105mm towed howitzers (total 54 tubes), supplemented by a general support battery equipped with eight 155mm towed guns. A six-man 60mm mortar section provides support to each infantry company. Four 81mm mortars (replacing the 4.2 inch mortar) are in each infantry battalion's combat support company.[7] The streamlined table of organization and equipment contains no tanks or other armored vehicles. It is of some significance to note that each soldier in the division will have night vision goggles.[8]

The capabilities of the light infantry division are to attack and defeat light enemy forces or seize terrain; conduct combat operations in contingency areas; reinforce forward deployed units; operate for 48 hours without external support; conduct military operations in urban terrain; conduct the rear battle; conduct air assault operations; and participate in

amphibious operations.[9]

In ***White Paper 1984***, "Light Infantry Divisions," Chief of Staff Gen. John A. Wickham Jr. states: "The British action in the Falkland Islands, Israeli operations in Lebanon, and our recent success in Grenada confirm that credible forces do not always have to be heavy forces . . . [it] will be deployable worldwide three times faster than existing infantry divisions . . . . [Light infantry will be] capable of bold, independent, decisive action . . . . It is important for all of us to recognize the geo-strategic value as well as battlefield utility of the light infantry division concept."[10]

It has long been recognized that getting to the global battlefield may be difficult. ***International Defense Review*** noted in a recent article: "Because it is painfully clear that there is a dramatic shortfall in USAF transport capacity at the same time as the growing need for reaction forces, the U.S. Army is in the process of redesigning its standard light infantry division into a leaner, more highly mobile and more firepower-intensive organization better suited for Rapid Deployment Forces."[11]

Hollingsworth, in his comments on the inability to "get there quickly," states that, "We have neither the air nor the sea lift to move even a fraction of the force. I cannot see how these divisions [heavy] and their equipment will ever be committed to battle. The facts are that the days of massive and slow buildup of forces through sea lift are over."[12]

In June 1948 the State Department presented a paper arguing that while war "is always a possibility," the main purpose in maintaining armed forces was to provide "support for our political position." Other purposes (of military forces) were to "act as a deterrent," to encourage other nations attempting to resist Soviet aggression, and to "wage war successfully if war should develop."[13]

That paper evolved into "National Security Council-68," a document that suggested the danger (as early as 1948) of limited war, of communist military adventures designed not to annihilate the West but merely to expand the periphery of communist domains, limited enough that an American riposte of atomic annihilation would be disproportionate both in terms of morality and expediency.

The prophecy of NSC-68 is as valid today as it was 30 years ago. The light infantry division will provide Clausewitz-like teeth for the political positions taken by our government. The creation of light infantry forces is timely, if not long overdue, if the United States is to create and maintain a position of strategic strength through flexibility.

The key, however, to the successful employment of the light infantry division is rapid deployment. Although an airborne or air assault division is considered light in comparison to a heavy division, it is important to understand that the airborne and air assault units still require twice as many sorties to be airlifted as the new light division. As "light" as the light infantry divisions will be, there still remains the question of getting them to global hot spots quickly. Hollingsworth is not the first nor will he be the last to warn of the inability of the United States to get forces to the battlefield. One could argue that it is even more important to get forces to the potential battlefield first. If we can extinguish the first sparks of war we will have accomplished our mission more completely than if we had to fight, full out. To paraphrase a famous Civil War quotation from Confederate Nathan Bedford Forrest, we must ensure that we can get the light infantry there—

"the firstest with the mostest." ★

Footnotes

1. Meyer, Gen. E. C., ***White Paper 1980***.
2. FC 71-101, "Light Infantry Division," p. 1-2.
3. Hollingsworth, Retired Lt. Gen. James F., "The Light Division," ***Armed Forces Journal***, October 1983, p. 85.
4. Velocci, Tony, "The New Light Division: Will It Work?" ***National Defense***, November 1984, p. 57.
5. Carney, Larry, "Mule Skinner Unit Considered for 10th Div," ***Army Times***, March 25, 1985, p. 29
6. Velocci, p. 57.
7. McNair, Maj. Gen. Carl H., Jr., interview in ***Army Times***, March 18, 1985, p. 28.
8. Velocci, p. 59.
9. FC 71-101, p. 1-6.
10. Wickham, Gen. John A., Jr., ***White Paper 1984***.
11. Lopez, Raymond, "The U.S. Army's Future Light Infantry Division: A Key Element of the RDF," ***International Defense Review***, Vol. 15, No. 2, 1982, p. 183.
12. Hollingsworth, p. 84.
13. Weigley, Russell F., ***The American Way of War***, Bloomington, Ind.: Indiana University Press, 1977. p. 379.

Maj. J. F. Holden-Rhodes was commissioned via the Platoon Leaders Class in the U.S. Marine Corps. Following instruction as a student officer at the Basic School, Quantico, Va., he served as a platoon leader with the 1st Battalion, 6th Marines, afloat in the Caribbean. He served as Aide de Camp to the commanding general of the 2nd Marine Division. In Vietnam he was assigned to 3rd Force Reconnaissance Company, 3rd Reconnaissance Battalion, 9th Marines and 3rd Combined Action Group; he served as a platoon leader, S2 and company commander. Following an interservice transfer he served with the 12th Special Forces Group. Holden-Rhodes is currently assigned as the Assistant Defense Attache, Kingston, Jamaica. He is attached to the 9001st, MID (Terrorism Counteraction). Writing under a grant from the Marine Corps Historical Center, he is completing a PhD program at the University of New Mexico.

MILITARY INTELLIGENCE DETACHMENT

MID(S)

Are We Destroying an Irreplaceable Asset?

Recent trends in the Army, particularly the Office of Personnel Management System and the new (renewed) emphasis on tactical intelligence, threaten to impair the effectiveness of a unique Army intelligence asset, the Military Intelligence Detachments(Strategic) program. This situation seems to be a result of ignorance about why MID(S) were originally formed, the great contributions they have made to national security in the past, and how their unusual capabilities can promote successful military operations today.

by Col. Robert J. Tata and Col. Lionel Simard

History of MID(S)

The MID(S) were formed in the Army's reserve structure after World War II, based on the experience of the Office of Strategic Services during the war. This experience clearly showed the Army's need for area experts in the conduct of worldwide military operations. General Donovan, director of the OSS, recruited area experts from the nation's universities and government agencies to tap their expertise in languages, history, economics, geography, political science, and other subjects relating to specific world regions. The Research and Analysis Branch of OSS combined basic area research with functional research and analysis, creating a new and valuable approach to strategic intelligence. (Corson, p. 172.)

"Notwithstanding the almost endemic rejection of intelligence which doesn't conform to already held, subjective beliefs, it should be emphasized that R & A's successful synthesis of capabilities and intentions analyses constitutes a truly unique aspect of that organization's performance, and is one which has failed to be duplicated in each of the postwar's attempts to organize the intelligence community on a national, centrally controlled basis." (Corson, p. 174.)

Evaluation of intelligence reports on possible hostile activities in foreign countries, logistic planning in theaters of operations, projections of resource needs, clandestine work requiring native language capabilities, bombing target analyses, and terrain and weather evaluations were typical jobs in which OSS area experts proved their worth. Donovan was so impressed with the accomplishments of these area experts that he was convinced of the nation's need to have continuous assets in strategic analysis. Most of his OSS structure was absorbed into the State Department after the war ended. (Smith, pp. 364-365.) The Army established units in the reserve structure, Strategic Intelligence Research and Analysis detachments, which later were renamed MID(S).

Development of Strategic Intelligence Detachments

The Office of the Assistant Chief of Staff for Intelligence implemented the Army's program for retaining a strategic intelligence capability. In 1947, efforts were started to recruit area experts by establishing Strategic Intelligence Research and Analysis teams at universities throughout the United States. Each unit was to arrange an "affiliation agreement" with a university or research institution. This agreement between the Army and the institution allotted an Army unit to the institution so that the institution's personnel could satisfy their military obligation in the unit, and the institution agreed to provide meeting space, access to libraries, and other facilities. In this way, OACSI sought to perpetuate the relationship of the military to the academic community, thereby preserving the capability of producing outstanding strategic intelligence. The following regulations were promulgated to ensure the professionalism and elite character of the MID(S):

- **MID(S) will be assigned missions to produce finished intelligence.**
- **MID(S) will be directly subordinate to OACSI.**
- **There will be stringent personnel requirements, including advanced academic degrees; excellent research and writing skills; civilian occupations related to strategic intelligence work; and university affiliation of unit commanders and other key personnel.**
- **MID(S) will be tasked with the production of strategic intelligence at the level of theater army and above.**

Some 65 MID(S) teams eventually were formed. Syracuse University, because of its Latin American studies program and the influence of Professor Preston E. James, was assigned three units—the 425th, 450th, and 454th MID(S). Dr. James, professor of Latin American geography, was the head of the OSS Latin American section from 1942 to 1945. Similar experts for Western Europe, Asia, Africa, the Soviet Bloc, and the Middle East were recruited in this nationwide effort to mobilize an ongoing strategic intelligence structure. Most of these units began to produce a series of studies called National Intelligence Surveys. The National Intelligence Survey was a classified compendium of the physical geography, cultural characteristics, political dynamics, and economic structure of individual countries. These and other intelligence products were considered major peacetime contributions to Army intelligence efforts. Five or six MID(S) were called to active duty during the Korean crisis; all distinguished themselves by immediately becoming operational on reaching the mobilization station. (Personal communication with retired Lt. Col. Robert Shafer.)

The success of the MID(S) program during these years is directly attributable to the professionalism of MID(S) personnel and their explicit recognition by OACSI. Retired Lt. Col. Don Edwards spent 24 years in the 425th; retired Lt. Col. Robert Shafer, a Latin American historian, spent 26 years in the same unit, 15 years as the detachment commander. Retired Lt. Col. J. McDowell was commander of the 454th for 17 years. Although this personnel tenure may seem excessive, it is reasonable since it does take many years to become an area expert. The active Army cannot afford the luxury of allocating personnel to such a "narrow" career; therefore, area expertise is a proper role for the reserve structure.

When MID(S) were under the direct control of OACSI, the personnel office and the office of the MID(S) coordinator at the Pentagon were always open to MID(S) personnel. For operations, MID(S) were authorized direct contact with Department of the Army level agencies; administrative matters followed normal command channels. Any operational problems or questions about career progress, nominations for detachment command, discussion of project assignments or other matters of mutual interest found concerned ears at the Pentagon. This provided a real "one Army" atmosphere. On April 1, 1974, management of the MID(S) program was switched from OACSI to U.S. Army Forces Command. Unfortunately, the quality of professionalism in the MID(S) program has since deteriorated. In theory, the same command relationships which existed before were to be continued. However, erratic and drastic swings in the management philosophy of personnel who now coordinate the MID(S) program at FORSCOM make the operations of that office unpredictable. Some directors have been unresponsive to appeals for the resolution of legitimate concerns. Commander appointments, unit reassignments, changes in command structure, and regulations governing MID(S) operations have been made in a secretive, seemingly capricious process. Management by fiat has seriously undermined the previous professionalism between the MID(S) and their managers.

Nature of MID(S)

At the present time there are 60 MID(S) with the following subordinations: Defense Intelligence Agency, 22; U.S. Army Intelligence and Threat Analysis Center, 19; Deputy Chief of Staff/U.S. Army Europe, 6; Foreign Science and Technology Center, 4; The Surgeon General, 3; U.S. Army

Japan, 2; Army War College, 2; and Western Command, 2.

To make the maximum contribution to their supported agency, the uniqueness and professionalism of the MID(S) program must be maintained. However, because MID(S) are atypical military units, their unique work and personnel needs are not appreciated by the "traditional Army mind-set." Historically, there has been conflict about the role of specialists versus the Army's concept of soldiers as generalists first, in the profession of arms. Army policy seems to display a split personality on this issue. Language training and the Foreign Area Officer Program seem to be acknowledgments of the Army's need for area experts. Yet promotion to general officer is virtually impossible for such specialists, and limited schooling opportunities and the turbulence of periodic reassignments preclude the development of true area expertise in the active Army.

Army OPMS policy now calls for a four-year limit of a MID(S) commander's tour, and there is talk of similar rotation for all MID(S) officers. The grade structure of a MID(S)—06, 05, 04, WO, E8, E7, E6 and E5—is unusually high for so small a unit. The purpose of this structure was to attract and retain highly qualified personnel. AR 140-192, Organization Training Assignment and Retention Criteria for Military Intelligence, Signals Intelligence, Electronic Warfare and Signal Security Units, is the MID(S) bible; it lists extremely high educational and occupational requirements for assignment to a MID(S) team. There have been as many as four doctor of philosophy degrees in one MID(S) team at one time. To do the job for which they were formed, the MID(S) must have personnel stability. The pool of qualified officers and enlisted has always been small, and is declining. We have recently seen officers appointed as MID(S) commanders who have no qualifications other than branch and grade, the most inconsequential of the requirements. We have also seen "good old boy" appointments in which personal contacts seem to supersede competence as a criterion for the position. The Army philosophy of a commander serving exclusively as a manager does not apply to MID(S) because their small numbers require them to be competent intelligence analysts if they are to accomplish their missions.

Present Need for Strategic Intelligence

Some years ago, we sat with several other MID(S) teams in a Pentagon briefing and were told by a representative of the Assistant Chief of Staff for Intelligence, "Strategic intelligence is dead; our only concern today is with battlefield intelligence." The concept of a quick future war, over within a week, is probably the assumption behind this thought. The short war philosophy, as a basis for allocating intelligence resources, is shortsighted and erroneous. From World War II to the present, we have been involved in many "conventional" armed conflicts but, thankfully, no nuclear war. In addition to this, the difference between tactical and strategic intelligence is not as sharp as it may seem. Knowledge about tribal animosities in Southeast Asia might be considered a piece of strategic intelligence, yet use of this information in combat could affect the outcome of a specific battle. It seems clear to us that peacetime preparedness must include knowledge about people and places which may become involved in future wars. Lack of knowledge about language, transportation systems, and location of civilian institutions in Grenada was a military embarrassment.

The reserve MID(S) program is the ideal place to maintain strategic intelligence assets. Is there any need for "in-house" area expertise? Couldn't the Army readily call on civilian area experts when the need arises? The prototype of a MID(S) member is a person with a little military training and a lot of area expertise? Active Army cynicism is sometimes heard: "This soldier can't be an intelligence reservist—his hair isn't long enough!" Nevertheless, the MID(S) program began to produce finished intelligence for active Army and Department of Defense agencies. After many unit citations and superior unit awards, the latest edition of AR 140-192, paragraph 3-2, finally states: "As their primary mission, MID(S) produce finished intelligence for their supported agencies during inactive duty training (IDT) and annual training (AT)."

We know of no other reserve unit which contributes directly to active military operations. In-house assets mean the Army has continuous access to dependable, professional, loyal and dedicated people who know their region of the world and have an appreciation for military operations. Occasional civilian consultants could not provide the timely and militarily thorough analyses which are the forte of MID(S) teams. What about the Defense Intelligence Agency, Central Intelligence Agency, the State Department, or other agencies with area expertise? One loud and clear conclusion of a study the senior author did as a mobilization designer for OACSI some years ago was that these other intelligence agencies do not fully satisfy the Army's intelligence needs.

Conclusion

The MID(S) are unique strategic intelligence assets; Army policy should explicitly and ungrudgingly recognize these differences, if there

is a need to maintain strategic intelligence production. Excluding "star wars," armed conflicts occur over human issues, they are fought by opposing armies which have their own unique cultural makeup, and they are fought in various places which also have unique characteristics. Reducing the unknown about the enemy, weather and terrain to a minimum is only part of the formula for military success. Detailed information about peoples, issues and places is another vital element in planning successful battles and campaigns. This is the province of strategic intelligence, a task for which the MID(S) program was devised.

If strategic intelligence needs exist, and the MID(S) are the appropriate assets to accomplish this mission, then Army policy should accommodate the uniqueness of the MID(S) program. Specifically, the following should be done:

- **Provide unit personnel stability. The function of the MID(S) requires recruiting and retention of top quality professionals. The pool of qualified people has never been very large and is decreasing, for a variety of reasons. There should be no assignment rotation for MID(S) officers, and if there must be one for commanders, the command tenure should be extended to six years. Rank structure now provides excellent career progression for officers, but enlisted ranks should be raised one grade for all lines.**

- **Adequate administration support by attachment to a larger unit must be institutionalized. Regulations state that at least 75 percent of MID(S) inactive duty training time must be allocated to the accomplishment of the unit's assignment research project. Various layers of administrative command levy increasing paperwork requirements. Unless units are assigned on orders to do MID(S) routine administrative work, they do the job reluctantly, or not at all. Infringements on MID(S) drill time that detracts from the research effort should be a topic for an Inspector General complaint. We have never known of a MID(S) commander who has resorted to this; commanders merely take the additional burden out of their own hides.**

- **Training opportunities and MID(S) assignments should reflect their intended results. Area expertise requires continuous involvement in study, travel, and research. Language training and training outside the continental United States should routinely be made available to MID(S). Hardly a "boondoggle," such training and assignments increase the value of MID(S) capabilities immeasurably.**

- **A unit should be designated a particular regional specialty and its assignments should always relate to that area. This will allow the unit to build true area expertise and their contribution to Army missions would be enhanced. Major Army commanders should not "play politics" and keep MID(S) assigned to them when there is need for their skills in other units. Perhaps a five-year review of Army needs and reassignments of MID(S) to support these needs should be instituted.**

- **U.S. Army Forces Command managers should re-establish an atmosphere of professionalism by opening up their management decisions to ensure input from MID(S) personnel.**

At a recent commanders' conference which included representatives from 19 MID(S), problems such as those discussed above surfaced; one of the solutions offered by active Army participants: commanders' initiative and ingenuity. Our position is that such "baling wire and chewing gum" remedies are destructive to the MID(S) program. If the asset is worth preserving, Army policy should be designed to nurture, not frustrate, it. On the specific problem of unit personnel stability, one colonel remarked, ". . . but your proposal would destroy OPMS." Our answer to him, and to you, is: what is the alternative—let OPMS destroy our strategic intelligence capability? ★

References

Corson, William R., **The Armies of Ignorance: The Rise of the American Intelligence Empire**. New York: The Dial Press/ James Wade,1967.

Lowenthal, Mark M., **U.S. Intelligence: Evolution and Anatomy**. Washington, D.C.: Praeger; Published with the Center for Strategic and International Studies, Georgetown University, 1984.

Smith, R. Harris, **OSS: The Secret History of America's First Central Intelligence Agency**. Berkeley: Universityof California Press, 1972.

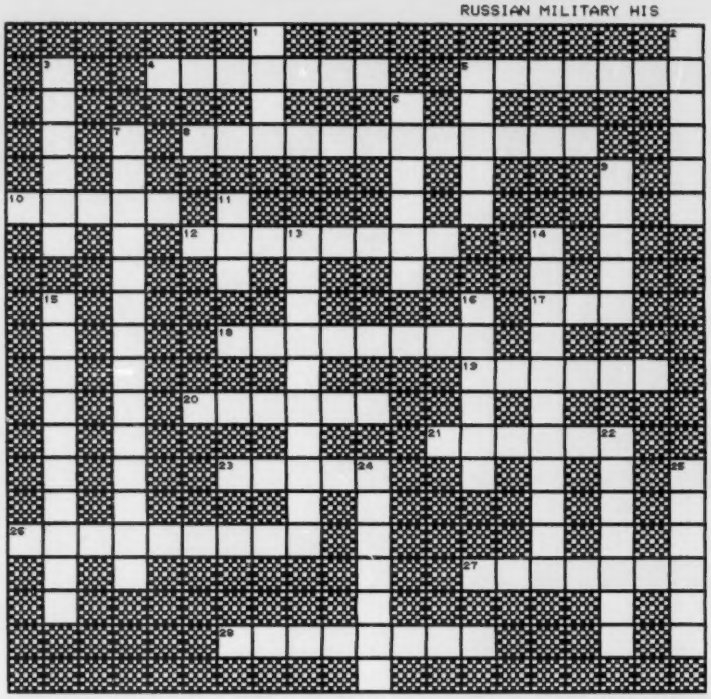
Col. Robert J. Tata is the commander of the 466th MID(S). He holds BA, MA and PhD degrees in Geography from Syracuse University and an MA in Economics from Florida Atlantic University. Tata is a graduate of the MI Officer Advanced Course, the Command and General Staff College and the Army War College.

Col. Lionel Simard is commander of the 454th MID(S). His education includes a BA from St. Anselm College, an MA from Middlebury College and a PhD from Cornell University. Simard's military education includes the MI Officer and Adjutant General Officer Advanced Courses, the Command and General Staff College and the Industrial College of the Armed Forces.

Crossword Puzzle

by Capt. Rudolph N. Garcia

RUSSIAN MILITARY HIS



ACROSS CLUES

4. IN 1799 THIS RUSSIAN FIELD MARSHAL DEFEATED FRENCH FORCES IN NORTHERN ITALY.
5. THE RUSSIANS FOUGHT THESE PEOPLE AS THEY ADVANCED TOWARD SIBERIA FROM 1643-1689.
8. SOVIET FIELD MARSHAL WHOSE THEORY AND DOCTRINE IN 1930'S INFLUENCE RUSSIAN ARMY TODAY.
10. HIS REFORM AND REORGANIZATION OF THE RUSSIAN ARMY FROM 1700-21 MADE RUSSIA A MAJOR POWER.
12. HIS OFFENSIVE IN 1916 ELIMINATED AUSTRIA-HUNGARY AS A MAJOR MILITARY POWER FOREVER.
17. IN 1938 THE RUSSIANS UNDER GEN ZHUKOV FOUGHT THE JAPANESE ALONG THE KHALKIN --- RIVER.
18. IN 1380 AGAINST THE TARTARS THIS WAS THE FIRST SIGNIFICANT RUSSIAN MILITARY VICTORY IN HISTORY.
19. HIS PURGE OF THE SOVIET OFFICER CORPS IN THE 1930'S WAS A PRIMARY CAUSE OF SOVIET DEFEAT IN 1941.
20. A FAMOUS COMMANDER OF RED ARMY FORCES DURING THE RUSSIAN CIVIL WAR.
21. DURING THE RUSSO- ------ WAR OF 1920, THE RED ARMY SUFFERED A DECISIVE DEFEAT AT WARSAW.
23. THE GREATEST TANK BATTLE OF WW2 ON THE EASTERN FRONT, JULY 1943.
26. THIS RUSSIAN CITY WAS UNDER SIEGE IN WW2 FOR 900 DAYS.
27. THIS SMALL COUNTRY FOUGHT THE USSR IN 1939 AND CAUSED 600,000 SOVIET CASUALTIES.
28. U.S. AND ALLIED FORCES TOOK THIS RUSSIAN PORT AND INVADED NORTHERN RUSSIA IN 1918.

DOWN CLUES

1. THE T-34 ---- WAS THE MAINSTAY OF SOVIET ARMORED FORCES IN WW2.
2. THE SOVIET ARMY DESTROYED 25 GERMAN DIVISIONS WHEN THEY DEFEATED ARMY GROUP ------ 1944.
3. FROM 1853-56 RUSSIA FOUGHT GREAT BRITIAN, TURKEY, FRANCE AND SARDINIA IN THE ------.
5. RED RUSSIAN FORCES DEFEATED WHITE RUSSIAN FORCES DURING THE RUSSIAN ----- WAR 1918-22.
6. THE MOST FAMOUS SOVIET FIELD MARSHAL OF WW2, CONQUERER OF BERLIN, SAVIOR OF MOSCOW.
7. WARSAW PACT FORCES INVADED THIS COUNTRY IN 1968.
9. THE SOVIET ARMY USES ----- BATTALIONS TO LEAD AN ATTACK OVER MINEFIELDS OR OTHER OBSTACLES.
11. THE 44TH --- WAS ONE OF TWO DIVISIONS DESTROYED BY THE FINNS AT SUOMUSSALMI, 1939-40.
13. THE TURNING POINT OF THE WAR ON THE EASTERN FRONT, NOV 42-FEB 43, WHERE GERMANS LOST 330,000 MEN.
14. SOVIET FORCES INVADED THIS COUNTRY IN DECEMBER 1979.
15. RUSSIAN FORCES WERE DECISIVELY DEFEATED BY THE GERMANS IN WW1, AUGUST, 1914.
16. THE RUSSIAN CITY THE GERMANS FAILED TO CAPTURE IN DECEMBER 1941.
22. SOVIET FORCES INVADED THIS COUNTRY IN 1956.
24. RUSSIAN ADMIRAL LEADER OF WHITE RUSSIAN FORCES ON EASTERN FRONT DURING RUSSIAN CIVIL WAR 1918-22
25. RUSSIA DEFEATED THIS BALTIC COUNTRY IN 1700-21 AND BECAME A MAJOR EUROPEAN MILITARY POWER.

(Solution on page 25)

9th Infantry Division (Motorized)

READY NOW!

by Maj. Robert Perceval

In October 1981, when the 9th Infantry Division (Motorized) received Gen. Edward C. Meyer's charge of "developing revolutionary approaches in tactics and equipment that can evolve into a new kind of division. . . ," few envisioned what has become the most dramatic program in the U.S. Army's 209-year history. To take a light infantry division and couple it with the most innovative off-the-shelf technology available, develop doctrine concepts and organizations, train soldiers, and complete the program by 1986 was by no means a small task.

To assist in this process, an organization called the High Technology Test Bed was formed. This organization was given the mission of interfacing with the 9th Division, industry, the U.S. Army Training and Doctrine Command, the U.S. Army Materiel Development and Readiness Command, and other agencies to assist in the 9th Division transition. The High Technology Test Bed, now called the Army Development and Employment Agency, continues this mission today.

The transformation and reconfiguration of the 9th Division were not focused on infantry units alone. The charter for change also encompassed aviation, engineer, signal, artillery, air defense, and military intelligence.

The division design for FY 84 is one which has changed and possibly will change in FY 85 with the advent of additional equipment. The FY 84 design includes three ground maneuver brigades consisting of five combined arms battalions (heavy), two light attack battalions and two combined arms battalions (light).

The heavy combined arms battalion is the mainstay of the division. These units will consist of two assault gun companies, one light motorized rifle company, a combat support company, and a headquarters company. Similarly, the light combined arms battalion will have two light motorized rifle companies, one assault gun company, a combat support company, and a headquarters company.

The light attack battalion is the most innovative new infantry organization. It is equipped with Fast Attack Vehicles, which will probably be similar in design to the commercial dune buggies now being used as surrogates. Each squad consists of two vehicles, one armed with an MK-19 40mm grenade launcher and the other a TOW. The elements will be used for deep attack combat operations or in various economy of forces roles.

The light motorized rifle companies will use the High Mobility, Multipurpose, Wheeled Vehicle as their primary squad carriers. These vehicles will carry the MK-19 grenade launchers.

The assault gun companies will provide the division with its primary ground anti-tank capability. Today, assault gun companies use the Improved TOW Vehicle; however, the M-551 Sheridan is the near future selection until other equipment can be evaluated.

The Cavalry Brigade (Air Attack) is considered a fourth maneuver brigade. The CBAA has two attack helicopter battalions, each with 21

AH-1S Cobra helicopters, a cavalry squadron of one ground and three light air cavalry troops, and a combat support aviation battalion of 36 Blackhawk helicopters.

The Division Artillery has three M198 howitzer battalions, each consisting of three batteries of six guns each. It also has one light artillery and rocket battalion with two batteries of 105mm howitzers, a battery of M270 Multiple Launch Rocket Systems and, finally, one target acquisition battery comprised of Q36 and Q37 radars.

The Division Support Command has three forward support battalions, one for each of the maneuver brigades. Additionally, there is a battalion to support the CBAA and a main support battalion which provides backup for the other support battalions.

Division air defense is provided by three direct support batteries of light air defense guns (12 per battery) and Stingers (16 per battery) to support each ground brigade. Innovations, such as the Avenger and Excaliber light air defense weapons, are still being considered by the 9th.

The engineer battalion has three DS companies and a light attack company designed to perform limited repairs to combat airfields.

The signal battalion has a traditional organization and a three-node support system to support the division area. At this time, secure means of transmissions, facsimile transmissions, and satellite communications are being reviewed.

The military police company will provide rear area security and prisoner of war control. The nuclear, biological, chemical company will provide the division with screening and chemical decontamination capabilities using new lightweight equipment such as the SANATOR chemical decontamination system.

In the division's new 14,500 soldier design, the military intelligence battalion and G2 section have assimilated the tools and personnel expertise to provide the intelligence-gathering capability to meet the needs of a fast-moving motorized force. A hand and glove military intelligence system has been developed which can rapidly acquire, analyze and evaluate intelligence information and data; provide it to the commander in the deep threat, main, and rear area; and also identify high payoff targets in the division areas of influence and interest.

"There are very explicit intelligence decisions which must be determined by us to maximize our available combat power," states Lt. Col. Gerald L. Schneider, 9th Division G2. "We must determine the enemy's strength and weakness, portray that situation vividly, and determine which targets to nominate in a target-rich environment. Also, determining the location of the enemy main attack, defense and delay positions and, finally, prioritizing our intelligence efforts will be key to our success. We must provide the commander the best information and recommendation so he can make those maneuver decisions which will be successful," Schneider said.

Intelligence decisions made by the G2 result directly in the information which paces the commander's maneuver decisions. A rapidly moving force commander must be able to select a scheme of maneuver and change it, if necessary. He must shift resources and priorities, establish a main thrust of maneuver, commit high leverage forces such as Army aviation, and determine priorities of effort. He also needs to determine if he should stand off or close with the enemy. The decision process is a tall order but is exactly what the division's new system is designed to accomplish from the perspective of intelligence, fire support, and maneuver decisions.

To aid the G2 section in providing commanders the most up-to-date real-time intelligence data for decision making, the military intelligence battalion also had to break the bonds of traditional thinking in fielding equipment, operational concepts, and training. A unique organization based on pacing factors for operational concepts has driven the evolution of the 9th Infantry Division's 109th MI Battalion.

Predicated on the premise that the 9th Infantry Division is designed to kill armor, the 109th must:

- **Predict enemy actions.**
- **Identify enemy mass.**
- **Provide high-value target data.**
- **Find weak points.**
- **Minimize risk.**
- **Deceive the enemy.**
- **Counter enemy communications.**

From those parameters the 109th MI Battalion's mission is fourfold:

- **Deploy C-141Bs for DS and GS missions in support of the division in Southwest Asia, but with utility in Europe and the Pacific.**
- **Perform intelligence and electronic warfare support missions.**
- **Exercise command and control of military intelligence battalion resources.**
- **Develop and evaluate new concepts, equipment and plans.**

According to Lt. Col. Patrick Hughes, the 109th commander and formerly the 9th Infantry Division G2, "The accomplishment of our mission is an ongoing developmental process. Our organization and equipment and, of course, our people have led the way to the most unique MI organization in the Army."

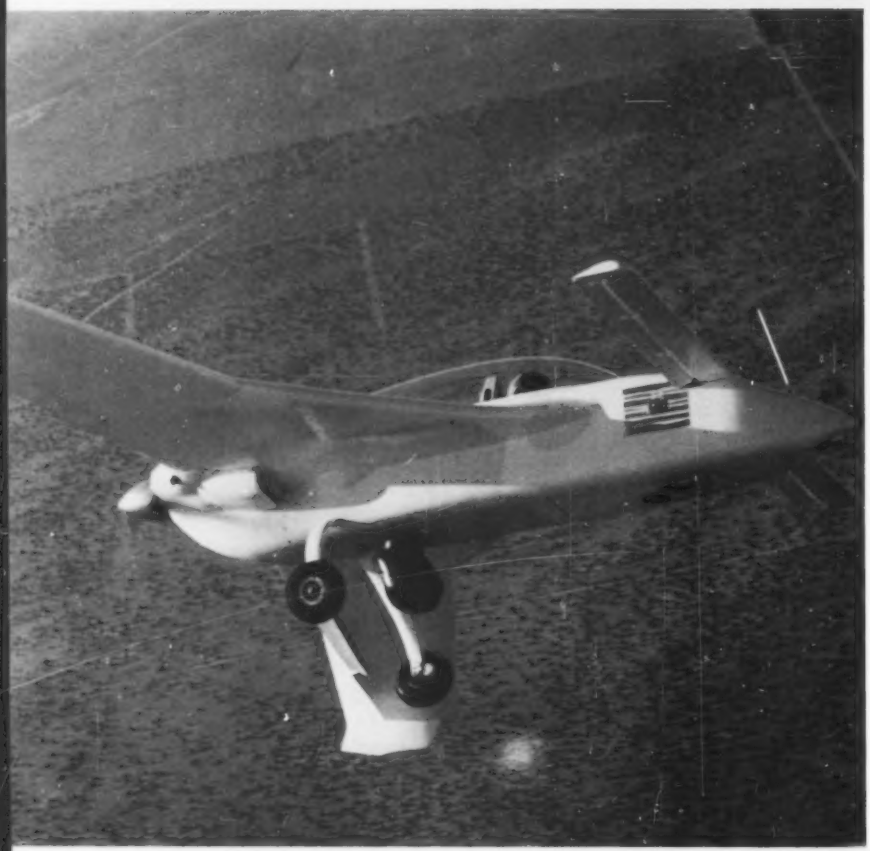
The organizational structure of the 109th MI Battalion is a slimmed down version of traditional MI functional elements, which have been organized for both direct and general support missions on a habitual basis.

The headquarters and headquarters company contains the battalion combat service support, the technical control and analysis element, and the interrogation and tactical deception elements. The tactical deception element provides technical deception support throughout the division area of operations, primarily in the electromagnetic spectrum, and also in the physical, visual and acoustic realms. The forward support companies, of approximately 60 soldiers, provide timely and direct response support of the enemy actions well forward of each of the three maneuver brigades.

The GS company, of some 100 soldiers, provides intelligence and electronic warfare across the division, to the CBAA in its role as a maneuver element, and for the rear battle, when required. A remotely piloted vehicle platoon in the GS company provides deep and near battle overhead real-time surveillance.

Finally, an 80-soldier airborne long-range reconnaissance and surveillance unit provides deep reconnaissance and surveillance.

"Our soldiers are organized to complete their missions and fight with the soldiers they usually train with in the



Remotely Piloted Vehicle "Mercury Green."

RPV Ground Control Station.

maneuver brigades," Hughes added.

"The MI companies know the maneuver commanders they work for . . . it's a team effort, more efficient and better controlled," said Schneider.

The organizational and operational concepts unique to the 9th Division were not developed overnight. "We began fielding the battalion on field training exercises Golden Blade and Golden Bow at the Yakima Firing Center in 1982. We progressed incrementally through FTX Laser Mace in 1983, CPX Caber Toss in the fall of 1983 and FTX Laser Strike in August of 1984," said Hughes. "This doesn't count the internal field tests and evaluations that were conducted. These events were on-the-ground testing with soldiers using developmental equipment and employing new operational techniques, not a laboratory situation," he added.

Through the course of its organizational development the 9th Infantry Division (Motorized) has looked at over 50 systems and pieces of equipment. "It is as important for us to know if a system doesn't work well as it is for us to know if it does work. If it doesn't work, it shows us the direction we need to go in," Schneider said.

Current developments in the MI arena span the entire spectrum—communications, computers, electro-optics and electronic intelligence. The division's capability has been enhanced with equipment like the AN/TRQ-32(V) direction finding system, the Watkins Johnson 9045 net control intercept system, the UAS-11 thermal imager, and the MSQ-103 ELINT intercept and direction finding system.

In the jamming area, low power jammers such as the RACAL 3100 and the Fairchild Applique and the hand emplaced EXJAM will take away the enemy's ability to communicate.

The long-range reconnaissance and surveillance unit using high frequency burst communications equipment, an all terrain insertion ability, and special Gortex clothing will provide extended clandestine intelligence to division planners.

The RPV with miniforward-looking infrared and daylight television will give the G2 and the division commander real-time confirmed intelligence.

Communications systems such as the PRC117 (SINCGARS forerunner) and the Litton DCT/LDCT (MI SMART) system of high speed digital data transmission will allow the passing of high volumes of intelligence on the future battlefield.

Test measurement and diagnostic evaluation maintenance and troubleshooting capabilities have also been reviewed and studied with great success at the MI battalion.

Efforts have continued to replace the carriers which will transport the downsized and more maintenance-free equipment provided to the 109th MI Battalion. Hydrostatically-operated carriers are currently being reviewed.

"Our inroads with MI SMART, the long-range reconnaissance and surveillance unit, the adaptation of a variety of sensors on an RPV platform, and the introduction of tactical deception skills and equipment into the battalion organization are the direction of the future," said Hughes.

"Key to our operational concept is that all of our systems link to the battalion automatic data processing and the division command and control system or MCS-2," he said.

"The MCS-2 is a divisionwide command and control system we are building using state of the art computer technology to automate division C^3I to provide our commanders, from battalion to the division level, the data upon which they can base decisions," said Schneider. The 9th Infantry Division is also integrating for the first time the initial phase of the all source analysis system (ASAS Interface Module Brassboard) with MCS-2. The all source analysis system uses all sources from the 109th MI Battalion as well as other division intelligence assets. The system employs microcomputers in four functional areas: collection management, target development, situation development, and C^2 integrated with a control and hand-off process to the C^3 system.

This is a brassboard effort at this stage and does not represent the total functionality of the all source analysis system, but only the key division tactical operations center support functions. As the brassboard evolves through the test bed, the MI battalion functions will be included until a full division-level all source analysis system can be demonstrated.

MSQ-103 mounted on Dragoon 300 surrogate.

Fast Attack Vehicles with TOWs and automatic grenade launchers.

The functions described below represent the first application software being developed for the brassboard effort.

Target Analysis

After receiving input from sources such as the division scouts, RPVs and other 109th MI assets, the computer assimilates data about enemy targets. With a direct communications link to the light weight TACFIRE terminal in the fire support element, immediate fires can be brought to bear on enemy targets if they are determined to be of high value. Targeting data is also provided rapidly in predetermined message formats and stored in a data base for future use, as the commander's fire support elements deem necessary.

Collection Management

The all source analysis system brassboard supports collection management by providing direction to the collective effort of all division intelligence assets. When gaps in situation development occur, the collection management function determines which is the best intelligence asset to task and then generates the tasking message. The focus is currently on assets under direct operational control of the G2 section, such as the RPV and the scouts. Information collected fills gaps in a pre-established template designed by the G2 according to the anticipated divisional needs. Data received by the G2 can be automatically transmitted to other users such as the brigade S2 section and Division Artillery for operational dissemination.

Situation Analysis

All information received in the main processor is also fed to three situation development terminals which determine the typical "situation map" presentation. An additional function is to develop the enemy courses of action.

Control Hand-off

The main processor directs all situation development intelligence to the control hand-off station, whereby it will be transmitted into the division C^2 system, the MCS-2. It also serves as a supervisor station over all other intelligence functions terminals. MCS-2 provides the commander all data pertaining to friendly unit (such as strength, logistic information and current disposition) and all the data available about the enemy situation as provided through the control hand-off. The system uses spreadsheet type charts, video graphics and narrative formats in a dual screen display to give the total picture rapidly and accurately in order to more quickly influence 14 locations distributed across the division battle area. These locations include the maneuver brigades, Division Artillery, the Division Support Command, and the air defense and MI battalions.

"That's why it is a system—in all its totality," Schneider said. "This development is a quantum improvement over anything else I have seen, and the first that really focuses on the commander's needs. It's the first attempt I've seen to integrate the combined functions of battle management." Schneider concluded by saying, "The 9th Infantry Division is certainly the most exciting unit I've worked with in the Army. We're continually improving the system, even though we're ready to use it now in its current state of evolution."

Soldiers of the 9th, using the most modern equipment, will continue to provide technology and operational direction to the U.S. Army. The unit is ready now and is designed to meet the threat armor challenge . . . and win! ★

Maj. Robert B. Perceval attended the University of Texas on an ROTC scholarship and graduated Distinguished Military Graduate in 1972 with a BA in English. He received an MA in 1978. He is currently the Public Affairs Officer for the 9th Infantry Division. His military schooling includes the Infantry Officer Basic Course, Airborne and Ranger Schools and the Public Affairs Officers Course at Fort Benjamin Harrison. He has served as platoon leader, executive officer, reconnaissance platoon leader and company commander in combat and combat support units. Perceval has served as an instructor for the basic and advanced courses teaching communicative arts and tactics at the Air Defense School, Fort Bliss, Texas. He also served as operations officer, Honolulu District Recruiting Command, Hawaii.

109th MI Battalion crest.

The 7th Infantry Division (Light)

A DIVISION IN TRANSITION

by Lt. Col. Thomas J. Sullivan Jr.

Although not targeted for implementation until October 1, 1985, the Army's first light division is well on its way to becoming a reality. Already, much of the Bayonet Division has made the transition from an "H" series infantry division to a "J" series light infantry division. However, its organic military intelligence battalion and its cavalry squadron have yet to test the "light" waters. This article provides a brief background of the division's journey over the past year and outlines events projected for the coming year, focusing on some of the employment concepts now being formulated by the G2 staff.

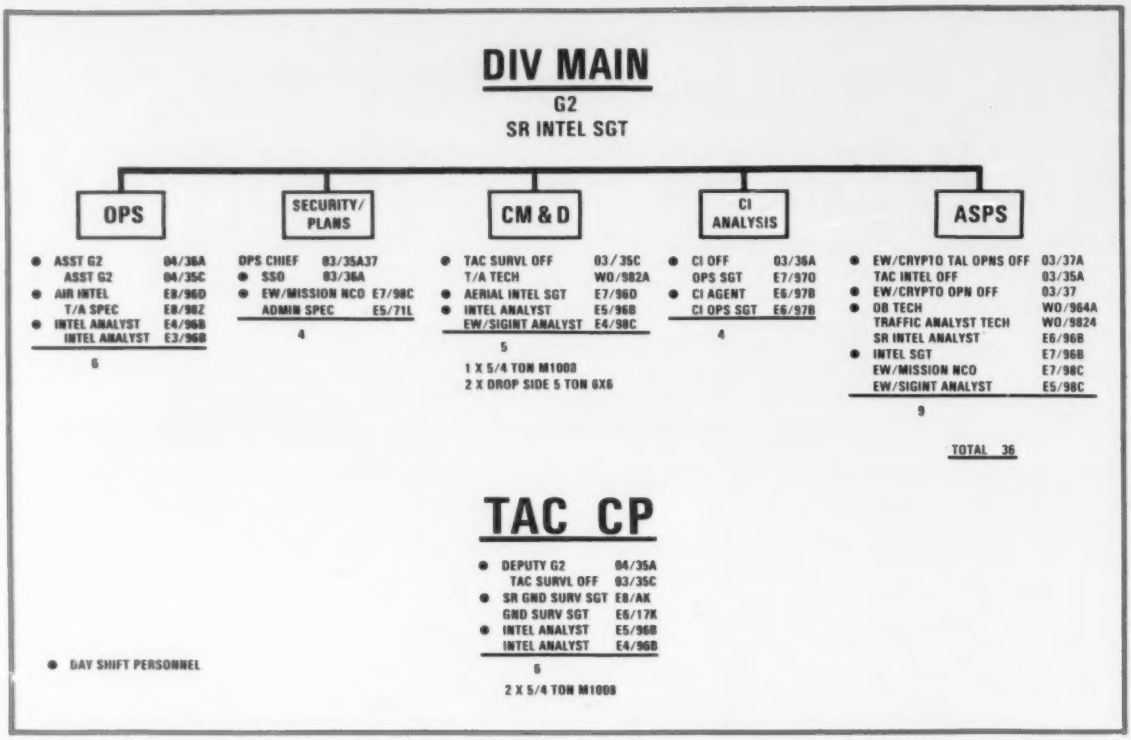
In the fall of 1983, the 7th Infantry Division was given the mission to become the first light division. Installation and division staffs immediately made an intensive study of the situation at Fort Ord, and then plotted the actions needed to bring the 7ID to its newly-designated organizational posture by October 1, 1985. The plan that resulted became the blueprint for events that have occurred over the last 15 months, as well as those projected through fiscal year 1986. Coupled with the basic blueprint was the guidance provided by Maj. Gen. James E. Moore Jr., then 7th Infantry Division commanding general. This invaluable guidance tempered all division associations with external units and agencies and led to the establishment of some ground rules. First, the 7ID(L) is not a test bed. That is the mission of other organizations. This does not mean, however, that the division would disregard innovative ways to accomplish the mission, but simply that the commanding general reserves the right to accept external equipment or concepts for testing. Second, the design of new tables of organization and equipment is also not the division's mission. Appropriate staffs merely recommend to the proper U.S. Army Training and Doctrine Command schools proposed designs based on documented data. Finally, the division is not in competition with TRADOC; it simply executes the force design directed by DA.

The restructure schedule was driven by three considerations: equipment availability, service support unit stability during the bulk of the transition, and the formation of new units after the conversion of established units. In the case of military intelligence, this schedule allowed the 107th MI Battalion to remain active by postponing its originally planned deactivation until the end of FY 85.

The following incident illustrates how strongly these considerations have shaped the division's operation. The division was told it was going to receive the UH-60 in the summer of 1985. This led to the natural conclusion that the 4th Quarter FY 85 would be the ideal time to restructure the aviation battalion and the cavalry squadron. Airframes and personnel that were UH-1 associated would be swapped for their UH-60 counterparts. It was also the last possible time to reduce the size of the MI battalion to that of an MI company. By keeping the battalion active until the last possible minute, the division could keep equipment and personnel to support any decision that would increase intelligence collection capability and provide support for contingency missions. The hope was that DA would see the effects of the cuts in the intelligence structure and take steps to rectify the original design. The division support command transition was also delayed because of the volume of lateral transfers, the influx of new equipment, and the dispatching of old equipment. The division could not afford to lose its materiel bookkeeper and maintainer in the throes of transition when it was most needed.

In October the division will be restructured under the "J" series table of organization and equipment, with items retained "in lieu of" replacements representing the only vestige of the "H" series configuration. FY 86 has been dubbed the year of certification. The scenario against which the Bayonet Division will be certified is in consonance with a White Paper issued by the Chief of Staff of the Army. The threat will be low intensity, escalating to the lower end of the mid-intensity spectrum. Therefore, all field training exercises for FY 86 will portray a guerrilla force that is reinforced late in the exercise by a regular army force of a hostile neighboring country.

For the most part, the original blueprint has been followed without alteration, with the Program Evaluation and Review Technique diagrams and their associated actions still intact. However, the MI battalion and the reconnaissance squadron are excep-



tions. These two organizations have given their commanders and division personnel challenges that still await solutions. The MI battalion status, along with proposed additions to the division's headquarters and headquarters company, has prevented the G2 staff and the battalion from solidifying garrison and tactical standing operating procedures for the light division. However, it has not prevented the conceptualization of how resources would be arrayed to perform the tasks outlined in FC 71-101, *Light Infantry Division Operations*.

It is obvious now that the people who man the new G2 staff will have to make accommodations. The new "light" G2 staff is 25 percent smaller than its "H" series counterpart, including the MI battalion division tactical operations center support element; however, it still has the doctrinal requirement to support three command posts; operations security; command, control, and communications countermeasures; and deception; as well as the normal intelligence and electronic warfare functions outlined in FM 34-1, *Intelligence and Electronic Warfare Operations*.

The TO&E authorizes the G2 section 36 people and major items of equipment. The diagram shows these resources arrayed in support of two tactical command posts operating 24 hours a day. Three points stand out: a rear command post is missing; the manning level on each shift is austere; and the mobility of the tactical command post is bought at the expense of the main command post. (Obviously, if the situation does not require a dynamic tactical command post, one of the vehicles would be returned to the main. It should be noted, however, that the return of one vehicle will not overcome the staff's constrained tactical ground mobility.)

The allocation of resources to the command posts shows the judgment calls that were made to achieve an intelligence operation that could support most of the requirements listed in the *Light Infantry Division Operations* field circular. To support the tactical command post and the main battle or current battle, the Deputy G2 and an analyst update the enemy situation and monitor the deep battle (forces that are not affecting the current battle). The enemy situation analysis is augmented by the ground surveillance radar NCO who is the tactical command post's collection manager and planner. His orientation is directed at ground surveillance, but he must also be able to request aerial surveillance through the division's main command post.

The total battlefield is the focus at the main command post. The G2 organization at the main reflects the organization described in FM 34-1, but with some accommodation based on light division constraints. The G2 operations branch, collocated with G3 operations, concentrates on the current and deep battle and provides a direct link to G3 operations. The security and plans branches perform doctrinal special security officer functions, provide administrative support to the all source production section whenever possible, and act as the G2's planning cell. It is in this section that the accommodation, alluded to earlier, starts to come into play. The SSO performs his or her primary duties and acts as the initial point of contact with G3 plans. In this role, the SSO alerts the G2 staff to the scope and timing of any upcoming opera-

tion and coordinates internally with G2 operations to identify the personnel who will do the detailed planning. On the night shift, the SSO addresses the situation in a slightly different manner. This officer's primary duty is planning, while SSO functions are secondary.

The collection management and dissemination section performs the classic functions of collection management and must execute this duty with the thoroughness of its larger "H" series counterpart. Therefore, some accommodation must be made to offset the reduced staff. The accommodation will occur as the CM&D section executes its dissemination function. Key items of information like the intelligence summary, situation updates, and RFIs will be the only items requiring staff journal entries. Positive control of every piece of information in the ASPS will not be attempted nor will those analysts be burdened with the responsibility of tracking every piece of data. The tactical SOP will identify reports that need to be tracked. The counterintelligence analysis section looks at the rear battle and monitors enemy intelligence capabilities. Its place of duty will be in the ASPS and the scope of its information will be all source. In this role, the CI analysts will be true planners for the G2 and G3. They will also recommend countermeasures and provide support to deception planning. Their placement at the main command post eliminates the rear command post as a place of duty for the G2. The ASPS will perform its doctrinal functions of intelligence analysis and production. Because of its austere manning, the CM&D section will get more involved, or more conscious of its role, as a disseminator of intelligence. The ASPS will also have to follow up on many actions that were previously handled by the CM&D section.

A retrospective comment is in order here. The manning and duties of the sections that compose the various command posts listed above may seem extreme in the context of a low intensity conflict. During the course of the lodgment and expansion phases of division operations, the duties described above are viewed as part of a worst case operational environment. However, the division's January command post exercise and March joint readiness exercise have allowed the G2 to confidently assess this alignment as one that would operate in a mid-intensity environment or in the initial phases of a deployment, when the pressure to resolve uncertainties is intense and immediate.

The weather team, along with other members of the G2 section, retains its "H" series structure under the light division. Its support role in a tactical setting can best be described as situation dependent. We expect to see forecasters (or observers) with any initial deployment to support air and ground operations. As the division establishes its airfield, the bulk of the support would be directed there. However, as the brigades expand their areas of operation or establish temporary forward operating bases, the weather team support will deploy to those locations. Command, control and support SOP still must be developed but the challenges to support light division operations seem within the weather team's capability.

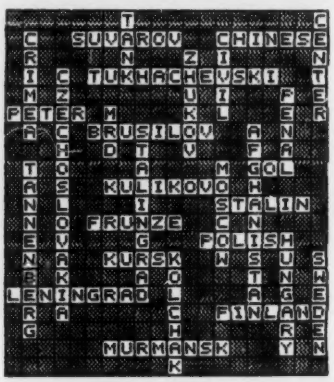
The terrain team, like the weather team, retains its "H" series composition. However, unlike the weather team, the terrain team was not included in the initial airflow calculations that generated the division's strategic sortie requirement. Therefore, it will perform the bulk of its mission during the predeployment phase of an operation. Mission support during the early stages of an operation will come from the team at Fort Ord through palletized or hand-carried products that are placed in the airflow. Once the division is established, the terrain team and its equipment will deploy.

Having described a deployment scheme for the weather and terrain teams, it is appropriate now to describe the complete intelligence support flow. Deploying with the first brigade task force would be the G2 tactical command post augmented by counterintelligence, prisoner of war interrogation, and signals intelligence personnel from the DTOC support element and a forecaster (observer) team. Their initial mission is to establish contact with the intelligence infrastructure in the country, support imminent combat operations, and build a data base for the remainder of the intelligence force. The MI battalion would provide a ground surveillance radar, counterintelligence, IPW, and signals intelligence task force to support the brigade. Rounding out this deployment package would be elements of the division's combat aviation brigade.

The long range surveillance detachment and the air and ground troops of the reconnaissance squadron weigh heavily in providing initial reports of enemy activity. Although mentioned last, their employment has always been considered an essential ingredient to light infantry intelligence operations. Their reconnaissance missions will be painstakingly developed by the G2 and G3 and executed by their commanders.

A close symbiotic relationship, born from the original reconnaissance squadron design, has developed into a team that gives the Bayonet Division confidence that it will be able to conduct combat intelligence operations in a low intensity environment. ★

Lt. Col. Thomas Sullivan is currently the 7th Infantry Division G2 and the Post Director of Security at Fort Ord, Calif. He is a graduate of the Officer Candidate School and the Command and General Staff College. He holds a BS degree in Engineering-Physics from Loyola College, Baltimore. Assignments include MI company executive officer; brigade S2; division special security officer, Vietnam; current intelligence analyst, J2, MACV; signals intelligence collection manager, S&T Directorate, DIA; and action officer, OACSI and OCSA.



Pegasu

The 312th M

A 900-mile road march from Fort Hood, Texas, to Fort Huachuca, Ariz., marked the beginning of FTX "Pegasus Expedition" for the 312th Military Intelligence Battalion (Combat Electronic Warfare and Intelligence), 1st Cavalry Division. The three-day exercise, which began April 14, provided the unit with an opportunity to test several new items of equipment and allow students of the U.S. Army Intelligence Center and School to observe an actual MI battalion in the field.

Sp4 Gregory D. Nicoson in Platoon Operations Center.

Ultradyne 60Kw generator.

Sp4 Dianna M. Kowalski with friend.

Sgt. Rene Zufelt operating MSQ-103A.

Sp4 Patrick D. Haynes with Libby 10Kw generator.

Photos by CW2 Roderick R. Spurbeck

us Expedition

MI Battalion trains at USAICS

The main body of the battalion left Fort Hood on April 10 in 107 vehicles, starting what may well have been the longest road march of any MI unit, and arrived at Fort Huachuca April 12.

"Pegasus Expedition" notionally portrayed the battalion supporting the "Mohavian Army" in a low intensity conflict scenario. During the exercise, the battalion tested three generators—the Ultradyne 60kw, the Quiet Reliable 30kw, and the Libby 10kw—all of which measured up to the claims of quiet performance.

At the conclusion of the exercise the battalion stayed in the field an extra day to brief USAICS students on site. On April 19, the unit moved into garrison and provided static equipment displays for additional classes.

The visit was not just characterized by a one-way flow of information; soldiers from the Intelligence Center briefed the battalion on new training procedures and equipment. Unit members also toured Southeastern Arizona, visiting the historic mining towns of Bisbee and Tombstone, and the border town of Nogales, Mexico, before starting another 400-mile roadmarch back to Fort Hood.

FTX "Pegasus Expedition" was part of a series of exercises in which MI units return to the "Home of Military Intelligence" to train in the desert environment and exchange information, ideas and experiences with the students and cadre of the Intelligence Center and School.

FINLAND'S SMALL SEAL

THE BATTLE OF SUOMUSSALMI

by Capt. Rudolph N. Garcia

On November 30, 1939, as Hitler prepared to invade Norway, Denmark, the Low Countries and France, the Soviet Union attacked Finland with approximately 500,000 troops organized into four Soviet armies totalling 26 divisions. Initially opposing this massive force were Finland's eight divisions numbering no more than 88,000 troops. (Finland would eventually mobilize 200,000 combat troops.) Stalin, fearing Nazi aggression and desiring buffer territory, wanted Finland to concede the Karelian Isthmus, various islands in the Gulf of Finland and the western part of Fisherman's Peninsula on the Arctic Ocean, and allow 5,000 Soviet troops to be stationed on Hanko Cape. "In all, Stalin wanted 2,761 square kilometers of developed Finnish territory in exchange for 5,529 square kilometers of undeveloped land north of Lake Ladoga."[1] After 45 days of tense negotiations, the patriotic, anti-communist Finns refused all Soviet demands. The territory Finland would have to give up would severely compromise its national security. Three days later the Soviets, accusing the Finns of attacking the Soviet border town of Mainila, invaded along the 900-mile Russo-Finnish border. G. I. Kulik, deputy people's commissar for defense, estimated the war would last 12 days and ordered Chief Marshal of Artillery Voronov to base all his operational estimates on 12 days.[2] Thirty-eight days after the Russo-Finnish War began, the Soviets suffered their greatest defeat of that war: Suomussalmi.

Initially, the main Soviet effort would be along the Karelian Isthmus; however, north of Lake Ladoga, they planned to cut Finland in half advancing with Gen. Chuikov's Ninth Army across Suomussalmi and the center of Finland to Oulu. This would cut Finland's supply line from "neutral" Sweden and Norway, take a major Finnish population center, and force Finnish troops to divert north from their main defensive positions along the Mannerheim Line in the Karelian Isthmus. Also, other Soviet armies were attacking to the north and south of the Ninth Army. Those armies, with objectives of their own, could provide support if needed. Essentially, it was a sound plan.

On November 30, 1939, the Ninth Army's 163rd Rifle Division crossed the border and advanced to Suomussalmi. The Finns, not expecting a major Soviet thrust in this barren wilderness, left the defense of this area to local border patrols and the Civic Guard. Two regiments of the 163rd advanced along the road from Juntusranta and the third regiment moved toward Suomussalmi on the road from Raate. By December 7 the Soviets had taken Suomussalmi. The Finns constantly harassed the Soviet columns but did not offer stiff resistance. They would wait for reinforcements. However, before retreating from Suomussalmi, they burned the village to the ground to prevent the Soviets from taking shelter from the cold winter.

With the 163rd at Suomussalmi, the road to Oulu was open. Only the Civic Guard and the border patrol, perhaps the equivalent of a battalion, stood between the Soviets and Oulu. Finally, on December 9, Col. H. J. Siilasvuo, commander of all Finnish troops in the Suomussalmi sector, arrived with the Finnish 27th Infantry Regiment from the 9th Division at Oulu. Unlike the motorized 163rd Rifle Division, the 27th was light infantry. They were equipped with only rifles, machine guns, tents and skis. Unfortunately, no artillery or anti-tank weapons were available. They were still on the train from Oulu.[3]

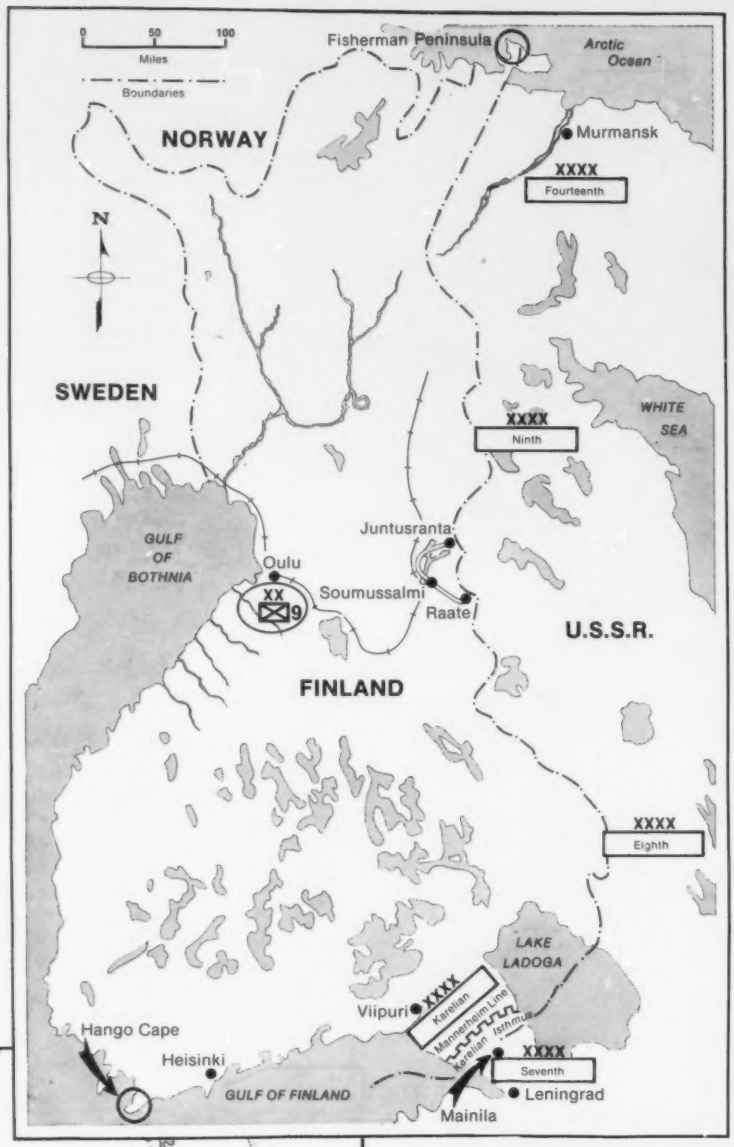
Siilasvuo commenced operations against the Soviets on December 11. Though not fully prepared to attack, the severe weather conditions prompted him to take offensive action as quickly as possible. The temperature, normally at minus 15 degrees Fahrenheit, fell to minus 40 degrees. Four feet of snow covered the ground. Although the Soviets had been attacking in the direction of the Haukipera Ferry, they had not moved from Suomussalmi in four days. The extreme cold severely affected their operations. Lacking the most basic winter survival equipment, such as tents, winter boots and skis, the 163rd, primarily a wheeled-vehicle unit, was dependent on the road for mobility and logistic support. Without skis in the heavy snowfall, the division could only patrol a few hundred meters to either side of Raate and Juntusranta Roads.

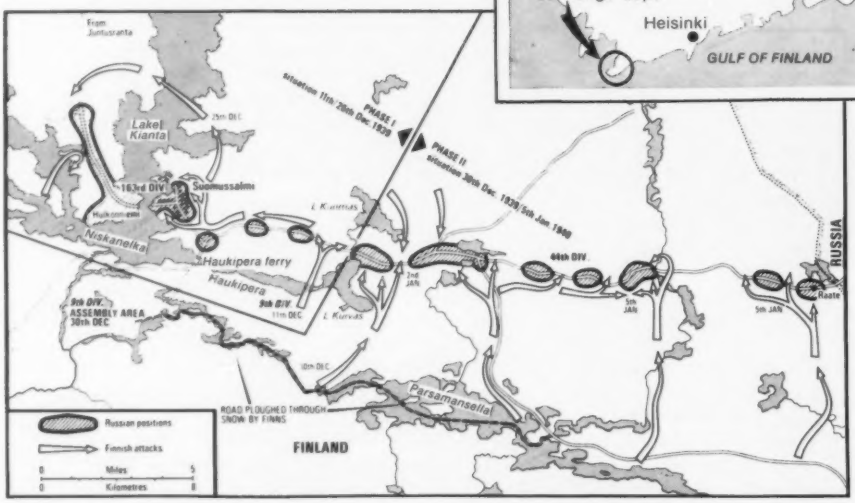
Quickly assessing the Soviet situation using ski-mounted reconnaissance patrols, Siilasvuo immediately took the initiative and attacked the Soviets from all directions. Siilasvuo's main body moved to cut the division's supply line and reinforcement route at Raate Road near Lake Kuomas. Simultaneously, other detachments were sent to cut the road to Juntusranta north of Suomussalmi and attack Suomussalmi itself. These attacks would break up the 163rd into *mottis*, or small, isolated groups.

"Motti means approximately half a cord of chopped wood which woodsmen measure and leave behind at certain distances, to be picked up later. In the winter war context, it meant an enclave of surrounded enemy troops."[4] Between the mottis, the ski-mounted Finns were able to move at will and coordinate their attacks against a separate motti or several mottis at once. Maj. Gen. J. W. Hagglund, commander of the 4th Finnish Army Corps, said motti tactics were not purposefully invented by the Finns: "People are talking about motti tactics as if the main objective of the Finns was to create them. This is not so."[5] According to Hagglund, mottis were developed as a result of their attacks against the Soviets and the Soviets' reaction to those attacks. In other words, it was the Soviets' 360-degree defense which prompted the formation of mottis. It was a natural reaction to an attack from all directions. The Finns became quite adept at motti tactics.

By December 12, following fierce fighting against Soviet tanks and repulsing Soviet counterattacks, the 27th Infantry Regiment cut Raate Road and any supplies to the 163rd. Suomussalmi, although repeatedly attacked, had not fallen, and Siilasvuo decided to call off all attacks against the town on December 18. His troops were exhausted, but the 163rd was broken up into several mottis and completely surrounded by his 5,000 men. Nevertheless, he realized that the Soviets were preparing for a breakout. Just as Siilasvuo was preparing a new attack, two batteries of artillery and two anti-tank guns arrived. With these reinforcements, he launched another attack against the 163rd, but was not strong enough to take Suomussalmi and destroy the division.

On December 22, 1939, Chuikov sent the 44th Motorized Rifle Division, an elite Ukranian unit from the Kiev Military District, to link up with the 163rd on Raate Road and open up the supply line to that beleaguered division. Only two companies of Finnish infantry held the road between the 163rd and the 44th. They held Raate Road between Lakes Kuomas and Kuivas for two weeks without significant reinforcements, and prevented the 44th from linking up with


0 50 100
Miles
Boundaries
Fisherman Peninsula
Arctic Ocean
NORWAY
Murmansk
XXXX
Fourteenth
N
SWEDEN
WHITE SEA
XXXX
Ninth
GULF OF BOTHNIA
Juntusranta
Oulu
XX
9
Soumussalmi
Raate
U.S.S.R.
FINLAND
XXXX
Eighth
LAKE LADOGA
Viipuri
XXXX
Karelian
Mannerheim Line
Karelian Isthmus
Hango Cape
Heisinki
XXXX
Seventh
GULF OF FINLAND
Leningrad
Mainila


From Juntusranta
Lake Kianta
25th DEC
163rd DIV
Suomussalmi
Niskanselkä
Haukipera ferry
Haukipera
9th DIV
11th DEC
9th DIV. ASSEMBLY AREA 30th DEC
10th DEC
ROAD PLOUGHED THROUGH SNOW BY FINNS
Persamanselkä
FINLAND
situation 11th-29th Dec. 1939
PHASE I
PHASE II
situation 30th Dec. 1939/5th Jan. 1940
44th DIV
1st JAN
5th JAN
RUSSIA
Raate
Russian positions
Finnish attacks
Miles
Kilometres

the 163rd. The two companies, with mortars and anti-tank guns, stopped several Soviet attacks and continuously harassed the 44th, deceiving the Soviets into thinking the Finns were at battalion or regimental strength. Gen. Vinogradov, commander of the 44th, "believed that a much larger force opposed him."[7] Had the 44th broken through the roadblock and linked up with the 163rd, the Soviets would have controlled central Finland and continued their attack to Oulu. The combined strength of both divisions, 35,000 men, would have been too large for the numerically inferior Finns to defeat.

With the 163rd surrounded and the 44th spread bumper-to-bumper over 17 miles of road, Siilasvuo regrouped to finish the destruction of the 163rd. On Christmas Day, the 9th Division's two reserve regiments, the 64th and 65th, arrived to reinforce Siilasvuo's forces. Finnish troops now numbered 11,500. Siilasvuo prepared for a concerted attack on December 26 from the west and north between Suomussalmi and Hulkonniemi. On December 24 and 25, just as final preparations were underway, the 163rd Rifle Division launched a massive counterattack. This counterattack forced Siilasvuo to postpone his own attack until December 27.

From December 27 to 29 an intense battle raged for Suomussalmi and Hulkonniemi. The Soviets, trapped in ever-shrinking mottis, continuously counterattacked to break out of their encirclement. Eventually, on December 28, Soviet resistance was broken, and the Soviets began to retreat from Hulkonniemi across Lake Kianta to Suomussalmi. Just as the retreating Soviets reached Suomussalmi, however, the Soviet troops garrisoning the town panicked and joined the retreat across Lake Kianta and to the northwest. The Finns pursued the Soviets on skis, and the Finnish air force attacked the fleeing Soviet division on the frozen lake. Toward the end of the day two-thirds of the 163rd Rifle Division ceased to exist as a coherent fighting force. They had frozen to death, been captured, killed or retreated to the safety of the motti, comprising the last third of the division. The next day found this fragment of the division completely surrounded. Only a few units were able to break out of the Finnish encirclement. The 163rd Rifle Division had been annihilated. "Left on the battlefield were 5,000 dead, innumerable others buried under the snow and there were 500 prisoners. The booty was impressive and made a welcome addition to the Finnish war effort. It included 25 field guns, 11 tanks, 150 trucks, 250 horses and huge quantities of rifles and ammunition."[8] The Finnish 27th Infantry Regiment, wet, frostbitten and exhausted, had been fighting for 18 consecutive days. Their victory, however, had been decisive.

"Though they had been stretched almost beyond the limits of physical and mental endurance, the Finnish troops were allowed no respite. After a few hours of rest they returned to the battle, this time against the 44th Division, which was now to feel the effectiveness of motti tactics.

"Motti tactics entailed a threefold process: reconnaissance and blocking, followed by attack and isolation and then by annihilation. Stage one had been completed while the fighting raged at Suomussalmi. Now, with its column strung out over the 20 miles of road as far back as Raate, the 44th Division offered a prime target for stages two and three."[9]

The 44th, however, was prepared for the inevitable Finnish attack. They were dug in along the length of the road, one-quarter mile to either side. They cut trees for cover and concealment and the division had their tanks prepared to counterattack down the length of the road. Despite these rigorous preparations, the Soviets would be defeated.

To apply the full mass of the 9th Division in the attack, Siilasvuo dug a road through the snow-covered lake two to three miles south of Raate Road. Using a truck with a snowplow mounted on the front, Siilasvuo had the 20-mile long road built while the final battle was being fought against the 163rd. Supplies, troops and vehicles were able to move along the road in preparation for the attack along the entire southern flank of the outstretched 44th Division. On New Year's Eve, the Finns attacked.

Initially, the Finns cut the head of the division from the main body, but Soviet resistance was very strong. On January 2, 1940, the Finns attacked another portion of the division with forces from the north and south; the Soviets counterattacked with tanks, infantry and artillery. The fighting was very bitter throughout the next three days, but finally, on January 5, a general assault along the length of Raate Road cut the 44th Division into several mottis. On January 6, four Finnish battalions were operating along the road and were concentrating their attacks against the Soviets with the remainder of the Finnish forces. The Soviet will to resist had finally been broken. They fled into the woods leaving countless dead and mountains of abandoned equipment. "Mopping up continued for several days, as the Finns hunted down half-frozen stragglers in the woods along the entire length of Raate Road and to the north. By the standards of that small war, the booty was enormous: the Finns captured 43 tanks, 70 field guns, 278 trucks, cars and tractors, some 300 machine guns, 6,000 rifles, 1,170 live horses and modern communications equipment which was especially prized. The enemy dead could not even be counted because of the snow drifts that covered the fallen and the wounded who had frozen to death. A conservative Finnish estimate put the combined Soviet losses (the 163rd and 44th Divisions) at 22,500 men. Counting killed, wounded and missing, Finnish losses were approximately 2,700 (only about 12 percent of these casualties were frostbite cases)."[10] By January 8 the battle was over. Two Soviet divisions, numbering 35,000 men, had been totally destroyed by a single Finnish division of 11,500 men. The Finnish army promoted Siilasvuo to Major General. The Soviet high command executed Vinogradov and several of his subordinates. The commanding general of the 163rd, Maj. Gen. Selendsov, was never heard from again.

Although numerically inferior, the Finns employed superior tactics and took advantage of the weather, the terrain and the Soviet failure to prepare for a winter war. The weather was extremely cold, averaging minus 15 degrees Fahrenheit on any given day. The Finns, however, were dressed warmly, were sent to heated tents every two hours if not in combat, and were equipped with skis. At night they slept in tents, and often hot tea and hot meals were available. Dressed in white smocks, Finnish troops blended well with the snow-covered

terrain. Moving on skis and lightly equipped, they could outmaneuver the Soviets with ease, attack at will, conduct reconnaissance patrols and disappear into the countryside. They also built improvised roads using horses and sleds: "A skier led a horse through the snow (in deep snow the horse proceeded by a series of jumps, which necessitated the rotation of the lead animals), followed by a horse pulling an empty sled, followed in turn by a series of horse-drawn sleds with progressively heavier loads."[11] Finnish ingenuity allowed their supply system to support their combat forces.

"In contrast, the Soviets were both cold and hungry. Finnish patrols deliberately sought out field kitchens as targets and eventually destroyed or captured all fifty-five of them."[12] The Soviets were not prepared for the extreme cold of Finland. The 163rd Division was Mongol and the 44th was Ukranian. The troops were not as accustomed to the cold as the Finns were. The Soviets, for the most part, did not have skis. Those that did, in the 44th Division, did not know how to use them. Consequently, the Soviets, equipped only with leather boots for summer operations, could not conduct effective reconnaissance patrols more than 400 meters from the road.

The Soviets were also bound to the road for supplies and maneuvers. The deep snow and severe cold prohibited off-road movement for wheeled vehicles. Worst of all, the Soviets did not have tents for shelters and often had to sleep by open fireplaces or dig into the frozen ground for protection from the elements. Eventually, however, with the large number of Finnish patrols, fires were forbidden since they would give away positions and serve as aiming points. Not equipped for winter war, the Soviets were at a distinct disadvantage. Their numerical and technical superiority was offset by the weather, the terrain and Finnish motti tactics.

The defeat of the Soviets at Suomussalmi, although tactically decisive, did not prevent the Finns from losing the war. Finland, a country of 30 million people, was hard pressed to win against the Soviet Union, whose population was 150 million. The Soviets, however, paid dearly for their victory over the Finns. "The most dramatic illustration of the price the Finns extracted was their annihilation of the 44th Motorized Rifle Division in January 1940. That battle is a classic example of what well-trained and appropriately equipped troops can accomplish against an enemy who has superiority in numbers and firepower but is not prepared for the special conditions of a subarctic environment. Such a region typically has dense coniferous forests, few and widely separated roads and a very cold climate—not a favorable setting for the deployment of standard motorized or armored units in winter. It is a realm where specially trained light infantry may prove its worth."[13] Eventually, 1,200,000 Soviet troops were committed to the Finnish theater of operations before the Finns surrendered.

Although 12,000 foreign volunteers fought for the Finns (among them were several hundred Americans), the Finns were desperately short on equipment, arms, ammunition and tanks. Had the Allies, Norway and Sweden supported the Finns with several divisions of troops and open lines of communication, they might have had a chance of winning. The arms shipments that reached the Finns from the Allies arrived too late to affect the course of the war.

Nevertheless, after Suomussalmi, the Soviets never again attempted to cut Finland in two. Most important of all, the victorious Finnish troops at Suomussalmi were committed to the battle for the Karelian Isthmus. Their presence helped lengthen the war by at least two months and was instrumental in causing 600,000 Soviet casualties.[14] Victory at Suomussalmi did not win the winter war, but it was "Finland's small Stalingrad."[15] ★

Footnotes

1. Richard W. Condon, ***The Winter War: Russia Against Finland*** (New York: Ballentine, 1972) p. 16.

2. Summarized from Eloise Engle and Lauri Paananen, ***The Winter War: The Russo-Finnish Conflict, 1939-40*** (New York: Scribners, 1972) p. 2.

3. Summarized from Condon, p. 82.

4. Engle and Paananen, p. 107.

5. Ibid.

6. Paraphrased from Maj. Gen. J. W. Hagglund as quoted in Engle and Paananen, p. 107.

7. Allen F. Chew, "The Destruction of the Soviet 44th Motorized Rifle Division," ***Fighting the Russians in Winter: Three Case Studies***, Leavenworth Papers, 5 (December 1981), p. 21.

8. Condon, p. 92.

9. Ibid.

10. Chew, p. 29.

11. Chew, p. 21.

12. Chew, p. 25.

13. Chew, pp. 17-18.

14. Casualty figure from R. Ernest and Trevor N. Dupuy, ***The Encyclopedia of Military History: From 3500 B.C. to the Present*** (New York: Harper and Row, 1977) p. 1055. This figure comes from a Finnish estimate of 200,000 dead and 400,000 wounded. Engle and Paananen state that Krushchev claims 1,000,000 Soviets were casualties during the war. Given the weather and terrain during the Russo-Finnish War, exact figures will never be known.

15. Col. Y. A. Jarvinen as translated by Engle and Paananen, p. 149. At Stalingrad from November 1942 to February 1943, the Soviet army, in a classic pincer movement, encircled and subsequently killed, captured or wounded approximately 300,000 Axis troops. Stalingrad was the turning point of the war on the Eastern Front during World War II. Although Suomussalmi was not the turning point of the Russo-Finnish War, it was similar to Stalingrad in the tactics used by the victor and the decisiveness of the results.

Capt. Rudolph Garcia is currently the commander of Company C, 1st School Battalion, U.S. Army Intelligence Center and School. He served for three years in the 302nd ASA Battalion and the G2 ASPS, V Corps, Frankfurt, West Germany, as EW platoon leader and company executive officer, assistant battalion S3 (operations), and assistant targeting officer. A 1978 USMA graduate, Garcia's military education includes the 37A and 37B track courses and the MI Officer Advanced Course. Before taking command, he was a Tactical SIGINT/EW and Military History Instructor for the Department of Tactics, Intelligence and Military Science, USAICS. An avid student of military history, Garcia is working to complete his MA in Military History at the University of Arizona.

TIPS for Countering Terrorism

by Lt. Col. Julian M. Campbell and Maj. Glenn E. Farrell

Internationally, U.S. military and civilian personnel continue to be viable targets for acts of terrorism. Therefore, it is essential that service members and civilians and their families take steps to protect themselves, their homes and their work places from terrorist acts. This article is designed as a quick reference to assist in the formulation of a strong personal anti-terrorism program. These counterterrorist tips have been applied effectively in Latin America. As U.S. involvement there continues, it can be postulated that terrorists will again select a U.S. target as they did in May of 1983 when an act of terrorism cost the life of a serviceman in El Salvador.

INDIVIDUAL SECURITY

No person is immune to the threat posed by terrorism. However, individual alertness, training and preparation for possible terrorist acts have proven to be effective deterrents to such acts. Thus, the likelihood of terrorist attack can be minimized by individual precautions which are consistent with the nature and degree of the terrorist threat, the mission of the unit and local circumstances. Every individual should become familiar with the general problem of terrorism, how terrorists operate and the procedures which are effective in reducing vulnerability to such acts. Generally, terrorists are most likely to be successful when their targets are lax in personal security measures and follow predictable daily routines.

CHECKLIST

PRECAUTIONS FOR INDIVIDUALS

- **Be aware that individual precautions can substantially reduce the probability of a successful terrorist act.**
- **Know what to do in emergencies.**
- **Vary travel routes and patterns; avoid personal routines.**
- **Keep families and office personnel informed of your itinerary and whereabouts.**
- **Be alert for surveillance; exercise caution with strangers; avoid casually giving out personal data such as addresses and telephone numbers.**

WORKPLACE SECURITY

To the terrorist, bombing is a psychologically rewarding, simple and relatively safe tactic, with great potential for generating terror and publicity. Types of bombs range from crude to very sophisticated devices. Most bombs, except those sent through the mail, have a time-delay fuse. Numerous detonators and methods of detonation are used in improvised explosive devices. Among the most used are remote detonators (commanded by wire or electronics); others include timed, pressure, release, or push-pull. It should be assumed that all bombs have an anti-tamper device. The use of improvised explosive devices by terrorists is only limited by their imagination.

In the context of planning for protection against terrorist bombing in an office or similar place of work, command or management personnel should follow a sequence of steps or phases, similar to those below. These steps should be repeated periodically:

- **Assess the threat of bombing and the vulnerability of the facility.**
- **Formulate policy and plans to cope with bombing, taking into account the differing characteristics of various portions of a base or facility.**
- **Implement the policy and planning with the necessary training of personnel, installation of required systems and devices and other security measures.**
- **Conduct both partial and comprehensive tests of all aspects of the effort.**
- **Evaluate and modify, if necessary, adopted policies and procedures.**

An assessment of the bomb threat should consider the following points:

- **Determine whether the facility has ever been the target of a bomb attack or received a bomb threat.**
- **Find out if similar facilities have been targets.**
- **Assess recent bombings, attempts or threats in the area: What was the target? Where was the device placed? How was it delivered? How did the bomber gain access? What device was used? What type fuse did it have? If a warning message was received, what information did it contain? Is there a pattern over several incidents? What security measures might have prevented the attack?**
- **Assess other terrorist activity locally.**
- **Determine if explosive materials have been stolen recently.**

The manner in which the assessment of a facility's vulnerability to terrorist bombing is accomplished and the amount of detail involved will depend on several factors, including the nature of the threat, size and function of the building and available expertise. However, the survey should be as thorough as possible and put into written form. It must be protected from compromise. In general, the vulnerability assessment should cover the following items:

- **Areas exposed to attack, and locations in and near the building where terrorists might conceal bombs.**
- **Damage that an incendiary or explosive device might do.**
- **Measures which can be taken to prevent a bomb attack and to minimize damage in the event that a device detonates or ignites in the target area.**

Experience has shown that there are four basic types of action which can minimize vulnerability to bomb attack:

- **Detection and warning against direct or stealthy assault.**
- **Denial of access to potential bombers.**
- **Identification and elimination, whenever practical, of potential hiding places for bombs.**
- **Physical protection of critical areas.**

CHECKLIST
DEFENSE AGAINST BOMBING

- **Does local protection planning recognize bombing as the most common terrorist tactic and provide specific measures to defend against it?**
- **Do protection procedures follow sequential steps or phases?**
- **Are procedures tested periodically?**
- **Have the threat of bombing and the vulnerability of the facility been assessed?**
- **Does the overall plan encompass physical security devices and procedures, necessary action in response to bomb threats, and procedures for search and evacuation?**
- **Does response to bomb incidents provide for appropriate reactions: (1) when a threat is received; (2) when a bomb or suspected bomb is discovered; and (3) when an actual detonation occurs?**
- **Do all individuals know what to do when they receive a bomb threat? Are bomb threat checklists available?**
- **Is everyone aware that they should never touch or move a suspected explosive device?**
- **Are adequate procedures established to control the receipt of hand-carried packages and other material? Has a package holding area been established?**
- **Are all personnel aware that they should check all mail they receive by looking, smelling, weighing and carefully feeling for any indication of explosive devices?**
- **Do individuals know what to do if they suspect the presence of explosives in the mail?**

CHECKLIST
MAIL BOMB RECOGNITION

Physical appearance of the envelope:

- **Oil stains ("sweating" of plastic explosive).**
- **Inks, particularly reds and blues, may bleed, staining the envelope.**
- **Use of extra sealing tape or string.**
- **Inner sealed enclosure.**
- **Peculiar odor.**
- **Wires, string or foil sticking out or attached.**
- **Feeling of springiness in the sides, bottom or top.**

Weight:

- **Heavier than usual for its size.**
- **Unevenly distributed.**
- **Heavier than usual for its class (for example, an air mail envelope weighing more than two ounces).**

Rigidity:

- **Greater than normal, particularly along its center length.**

Thickness:

- **Not uniform, or with bulges.**
- **For medium size envelopes, the thickness of a small book and fairly rigid.**
- **For large envelopes, bulkiness, an inch or more in thickness.**

Address:

- **No return address.**
- **Hand printed.**
- **Addressed to a high ranking officer either by name, rank, title or department within the organization.**
- **Title or rank for the officer is incorrect.**
- **Poorly typed or handwritten.**

Writing:

- **Marked (written or stamped) personal, confidential, private or eyes only.**
- **Marked (written or stamped) air mail, registered, certified or special delivery.**
- **Misspelled words, particularly those in common military usage.**
- **Style of writing is foreign.**

Stamps:

- **More than enough postage for the piece.**

Postmark:

- **Foreign.**
- **From an unlikely city or town.**

VISITOR COUNTERMEASURES IN OFFICE AREAS

Always monitor visitors to your office area. Keep a visitors' log and require all visitors to sign in. This gives you a handwriting sample. Also, place the log so the visitor has to lean over toward you—this gives you a chance to do some visual "frisking." Watch the belt for sharp bends which might indicate a concealed weapon.

Watch briefcases carefully; they can contain virtually anything. The visitor should hold the briefcase on his or her lap, and open it there. The visitor should not be allowed to open a briefcase on a desk.

If visitors are carrying packages, have an area designated for placing such items (keeping in mind safety, should they explode). Pay particular attention to unexpected delivery of items. Do not allow the item to be left until you determine: Where it is from; who sent it; whether the delivery person is certain he or she has the right address; and what is supposed to be delivered.

Be wary of a delivery person who uses a ruse to leave the package behind, such as going back for something left in the vehicle or to check the address. Never attempt to examine a suspicious looking package or box yourself. Call the nearest explosive ordnance disposal or local military police.

Remember that terrorists commonly work in pairs—male and female; and beware of the visitor who appears to be "looking around." All visitors should be requested to show some form of identification, including persons in military or police uniforms.

VEHICLE AND TRANSPORTATION SECURITY

Individuals are vulnerable when on the move and probably most vulnerable when entering or leaving residences. At such times, because of preoccupation with their purpose or with driving, people may be generally off guard; hence they should take extra care to be alert for indications of trouble—particularly when driving a vehicle obviously identified as a military vehicle.

The times and routes of travel to home or any other routes regularly traveled should be varied. Even though your car is marked, you may want to consider trading off to avoid using the same car every day.

Before leaving home or work, people should make a habit of checking the streets for suspicious individuals or vehicles. When driving, use well traveled streets.

Vehicles should be well maintained. Where possible, use a locking gas cap, inside hood locks, a fire extinguisher and a first aid kit. Consider having at least three rear view mirrors.

If you are being followed, it does not necessarily mean that an attack is imminent. Terrorists usually watch their intended victims for some time before attacking to determine the victim's routine and evaluate his or her security.

If you think you are being followed, attempt to verify the fact by deviating somewhat in a normal manner from the planned route. Also, take down the make, color and license number of the vehicle following and the number and description of occupants. If surveillance is confirmed, do not complete the trip as planned but travel to the nearest safe haven such as a police facility. Do not drive home. Do not stop. Try not to let the followers know you are aware of them.

If you are being attacked, or if you believe the surveillants are going to attack you:

- **Make a relatively high speed turn in either direction, even if it means jumping curbs or traffic medians. Impact with curbs should be at low speeds (35 mph maximum) and at an angle (30 to 45 degrees). Prepare for a jolt.**
- **Keep vehicle moving at all costs, regardless of condition; for example, despite a flat tire or disabled cooling system.**
- **Avoid being boxed in or slowed down by other vehicles. Where possible, drive in the center of the road for maneuverability.**
- **Keep windows closed—this should be done routinely anyway.**
- **If a firebomb is thrown, drive away at a high rate of speed. Otherwise, wait 10 seconds and abandon the vehicle on the opposite side of the fire. Fire bombs normally burn out within a few seconds.**
- **In the event of shooting, duck below the window line and stay low. Commonly used 9mm and .38 caliber bullets will penetrate the automobile body; however, the bullet may be deflected and its force reduced.**

CHECKLIST

PARKING:

- **Always lock vehicle.**
- **Do not leave vehicle on the street overnight, if avoidable.**
- **Never get out without checking the area for suspicious individuals—if in doubt, drive away.**
- **Leave only the ignition key with parking attendants (separate the ignition key on key rings).**
- **Do not permit entry to the trunk unless you are present.**

DRIVING:

- **Before entering vehicle, examine it for any suspicious, unexplained objects—strings around it or inside of it or underneath. Look for evidence of attempted entry. Suspicious objects should not be touched. Call for assistance.**
- **The gas tank of your vehicle should be kept at least half full.**
- **When vehicle is moving, seat belts should be fastened, doors locked and the windows closed.**

HOME SECURITY

Protection of the family and home presents variable conditions and unique psychological problems which make home protection the most difficult area in the entire security program to manage. Teen-agers are a particular problem as they tend to resist strict routines and close supervision. Not only must personal consideration be taken into account, but the home security plan must also answer questions of fire, medical emergency and natural disaster. The primary purpose of the home security program, including plans, safety equipment and alarm systems, is the personal safety of the member and his or her family. A comprehensive home security program will concentrate on making the home target too "high risk," thus directing the terrorist elsewhere.

Kidnapping and terrorism are painful battles of nerves and stress, and most terrorists are psychologically better prepared than is the member's family. The solution to this form of crisis is basically twofold: training the family to be a strong psychological unit, especially under stress; and establishing a home security program that is based on proven security principles and hardware, and reinforced with dedicated family participation. Not only must the entire family voluntarily be motivated to accept security restrictions, but they must closely adhere to the routine and details of these restrictions. The preliminary step in developing a home security program is an in-depth security survey, with both husband and wife present. This survey can be conducted by the law enforcement activity's physical security section.

Individual family members must understand that they are part of and contribute to the home security program. Security awareness is one area that is normally very weak; yet, every family member can develop a special sense for observing his or her surroundings and spotting potential security problems. All members of the family should become inherently aware of the following everyday situations and recognize their potential danger.

- **When a child is to be picked up at school, the school should have an established procedure with which to verify this action with the home or office.**
- **When calling about an emergency situation always give your name and then your location. Next, proceed with an explanation of the problem.**
- **Terrorist victims are normally under surveillance for a number of days before any action takes place, so be aware of possible surveillance activities.**
- **Stairs are isolated areas and should be avoided if elevators are available.**
- **Consider telephones as possibly being electronically compromised, and limit the amount of information given out. Always answer the telephone with "hello" and establish the identity of the caller before giving such information as your name, address and who is at home. Unrecognizable callers identifying themselves as "old friends" and "business associates" should be referred to the member's business telephone number.**
- **Family members should never unlock doors or permit entry of strangers. Service or maintenance personnel should be verified by telephone with their respective companies before they are allowed to enter the residence. If forced entry is attempted, the family should retreat to a safe room, if available, and notify security personnel.**

The special problems of home security are many, and the need for a good security program with contingencies to meet specific terrorist threats cannot be overemphasized. The above concepts can help build the psychological framework for stronger family security involvement.

The tips presented in this article are by no means all inclusive, as there is no absolute protection against acts of terrorism or crimes of violence. Additionally, these protective measures must be tailored to various parts of the world and to the nature of the terrorist threat. These security measures are intended to help minimize the risk of an incident by providing a "before the fact" awareness of actions that can be taken to prevent, reduce or delay a terrorist act. Security awareness and common sense coupled with these counterterrorist tips could save a life. ★

Lt. Col. Julian M. Campbell was commissioned in the Military Intelligence Branch in 1965. He holds a BS in Political Science from Virginia Tech and an MS in Human Resource Management from the University of Utah. He has commanded the 503rd MI Company, 3rd Armored Division; served as G2 Plans Officer, XVIII Airborne Corps; and served as an author/instructor at the U. S. Army Command and General Staff College. Campbell completed numerous counterintelligence assignments in Vietnam, U. S. Army Europe and CONUS. Prior to assuming his current position as Commander, 2nd School Battalion, 1st School Brigade, U. S. Army Intelligence Center and School, he was the G2, 193rd Infantry Brigade (Panama).

Maj. Glenn E. Farrell, USAR, holds a BS in History from Western Michigan University, an MS in Education from Long Island University and an MS in Criminal Justice from Nova University. He is a graduate of the Military Intelligence and Military Police Officer Advanced Courses and the Marine Corps Command and Staff College. On active duty, he has served as an MP officer at West Point and in the Republic of Panama. Currently, he is assigned as Chief, Plans and Training Division, G2, 193rd Infantry Brigade (Panama).

Computers
A Counterintelligence Concern

By Maj. N. Glenn Blackburn

Computers have become our nation's "dumping ground" for large amounts of highly classified defense information. They have become the high-tech vaults of our era, just waiting to be cracked by a determined hostile thief. As valuable as these tools are, they have made the Department of Defense dangerously dependent upon vulnerable worldwide computer systems to process and store classified data on personnel, logistics, air defense, command and control and intelligence systems. Melville H. Klein, director of the DOD Computer Security Evaluation Center, acknowledged in a recent article: "Our command, control, communications and intelligence posture is critically affected and dependent on computers."[1]

DOD dependency on C³I computers was illustrated by an automated failure within the Worldwide Military Command and Control System: "In November 1979, the WWMCCS was being tested in a simulated alert and somehow several of the computers in the WWMCCS network interpreted this test as an actual national crisis."[2] For a moment, the WWMCCS Honeywell Computer System was in complete control and commanded the Strategic Air Command to prepare armed nuclear B-52 bombers for flight. Fortunately, someone identified the combined human and computer error, and a country that was on the "striking edge" of war was returned to normal operations. "In June 1980, this episode was repeated three times under varying circumstances."[3] Were these incidents accidental or manipulated by someone? A continued proliferation of computers throughout the armed services will force top military leadership to rely on computers to activate early warning systems and to assist in the defense decision-making process.

Rapid growth in the use of computers has far surpassed present day technology to safeguard stored data. A recent article in ***Data Security Management*** warns: "Since no hardware manufacturer can guarantee data security, the primary responsibility falls on the user."[4] Lt. Col. Nick Babiak, who served as the Air Force's principal advisor for Computer Resources, observes: "There is no computer system today within the government that is totally secure from unauthorized penetration or manipulation."[5] The problem of computer security within DOD can be depicted by the following counterintelligence model of vulnerability:

(T)HREAT + (D)EPENDENCY +
(L)ACK OF SECURITY ÷
(C)OUNTERMEASURES =
(V)ULNERABILITY

This model of vulnerability must be divided by an effective countermeasures program that will protect our automatic data processing systems from hostile penetration and attack.

ADP centers containing classified defense information offer the hostile agent a prime target for clandestine collection or sabotage. An intrusion can be accomplished in a number of ways.

Penetration of Master Program. The most severe threat to any ADP system is the seizure of the master program (also known as the executive program). If penetrators can seize control of a master program, they can control the entire system.[6]

Deception. Using their own computer equipment, penetrators masquerade as legitimate users. In order to succeed, they must have access to system procedural guides, if proper hardware and software security controls are built into the system.[7]

Wiretapping and Eavesdropping. Intruders simply tap lines between terminals and install their own equipment to monitor all computer traffic. Eavesdropping may involve the detection of acoustic data and, thus, the use of a parabolic microphone from a distance; observing a display with binoculars; wiretapping a communications line; or listening in on radio or microwave communications.[8]

Circumvention. Penetrators attempt to circumvent security controls by probing for "trap doors" in the system that will allow entry without going through prescribed security controls.[9]

Theft or Compromise of Printed System Documentation. Penetrators physically steal classified documents such as authenticators or passwords. This would require a breach of physical protective measures, or the help of systems personnel who have been subverted or bribed.[10] The hostile agent may attempt to subvert, blackmail or recruit personnel who work in the facility to collect information, manipulate programs, and act as the agent's "eyes and ears" within the facility.

Browsing. Legitimate system users attempt to gain access to classified files for which they have no authorization. Individuals who have Confidential security clearances browse through the system until they enter an unauthorized Secret file.[11]

Between-the-Lines Entry. A penetrator who has tapped into the communications line waits until a legitimate user is finished but has not signed off the computer, seizes control of the lines, and acts like a legitimate user.[12]

Logic Bomb. A logic bomb is a computer program which can be executed at appropriate or periodic times that "sets the computer up" for the commission of an unauthorized

act.[13] An agent who has penetrated the system could plant a logic bomb which could cause a complete system breakdown in a wartime emergency.[14]

Trojan Horse. An agent places a secret instruction in the software that is activated under special circumstances. Once a Trojan Horse is in place, it is likely to remain hidden even from the most skilled experts.[15]

Piggyback Entry. After tapping into the computer terminal lines, a penetrator can intercept data being transmitted to a legitimate user and substitute false data in its place.[16]

Sabotage. "Sleeper" agents who have blended into the mainstream of society could be issued orders to sabotage critical DOD computer facilities prior to or during hostilities. The agent could physically attack power sources, air conditioning systems, and water supplies. Although access to such facilities is tightly controlled, few installations are hardened to withstand the effects of well-placed, high-explosive demolitions.[17]

Technology Transfer. Recent Soviet acquisitions of Western computer technology have made our military-related computer systems even more vulnerable. More than one-third of all known Soviet integrated circuits have been copied from U.S. design. Not only do they copy our systems but they also study them to determine system vulnerabilities and techniques of exploitation.

DOD computers, by virtue of their importance to military decision making and our dependency on inadequate mechanical security devices, are high-priority targets for the covert agent's intelligence collection and sabotage plan. A determined enemy will attempt to disrupt our communications and decision-making process by attacking our C³I systems, and computers are a vital and integral part of those systems.

On an optimistic note, the government is committed to correct known security-related management problems in federal ADP installations. The Army's 902nd Military Intelligence Group, Fort Meade, Md., has made significant progress in improving computer security. Evaluation teams are dispatched to assist units in developing computer security programs.

Typical security problems are:[19]

- Insufficient emphasis on computer security.
- Lack of vulnerability, threat, and risk assessment.
- Lack of management involvement in computer security issues.
- Lack of an overall computer security program.
- Lack of balance in computer security personnel.
- Inadequate security planning.
- Inadequate contingency planning.
- Open-shop computer centers, having no access control procedures for personnel.
- Lack of computer system access controls.
- Inadequate supervision.
- Inadequate division of responsibilities.
- Untidy operations.
- Poor documentation and untidy programming practices.
- Lack of program certification procedures.
- Inadequate security training.
- Low employee morale.
- Excessive processing error rates.
- Lack of input and output controls.
- Lack of protection against fire, flood, or natural disasters.
- Failure to eliminate fire hazards.
- Lack of enforcement of security policies and procedures.
- Lack of contingency plan testing.
- Lack of internal audit of security aspects.

DOD security policies, directives, and procedures have been written and continued research efforts are directed toward solving the mechanical security problem. Ongoing research is being conducted in coordination with the following professional organizations:[20]

Carnegie-Mellon University. Sponsored by the Advanced Research Projects Agency, the HYDRA project will develop a multiprocessor computer from a minicomputer base. A major portion of this effort is devoted to the development of a secure operating system kernel named HYDRA.

Lawrence Livermore Laboratory. Research in Secure Operating Systems is devoted to the development of systematic methodologies used in testing the security of computer operating systems.

Stanford Research Institute. Research effort is devoted to the development of a demonstrably secure kernel for operating systems and to the analysis of computer abuse.

Case Western Reserve. Research is devoted to information protection concepts and the structuring of hardware and software systems.

Cornell University. Research concerns the applications of privacy controls to data base management systems.

IBM Corporation. The Research Security System Project involves the installation at four sites of a special version of OS/360 MVT by the IBM System Development Division. The purpose of the study is to test security systems in a live user environment. The IBM Research Division is engaged in several projects concerning computer security, user identification techniques, and hardware encryption.

Air Force Electronics Systems Division. Research is devoted to the development of security features in Air Force computer systems, including the establishment of security requirements and system changes required for the Honeywell Multics System installed at the Pentagon. The MITRE Corporation is working with the Air Force in developing a certifiably secure kernel for the Honeywell 6180 Multics Computer System. Additional effort is devoted to the development of prototype secure data management system for the PDS 11/45.

TRW Systems. TRW is participating as a data security study site in the IBM RSS Project. TRW is also developing security requirements, procedures, and automated test and evaluation aids for systems security certification. TRW has developed data management systems with separate control of access to files, records, fields, and even field values. Additional efforts include the development of a computer security manual for the Air Force and a secure operating model for an advanced Control Data Corporation product line.

National Bureau of Standards. The National Bureau of Standards is developing standards, policies, guidelines, and technical solutions for data security in the government ADP community. The National Bureau of Standards also provides a forum for the analysis of privacy issues and formulates guidelines for achieving national coherence in legislation and regulations dealing with privacy.

Honeywell Information Systems. Honeywell is the primary contractor for WWMCCS, which uses the Honeywell General Comprehensive Operating System computers. Honeywell is attempting to secure the Multics System for use in military multilevel security applications. Additional research is being directed toward problems of encryption, personal identification, and related topics.

Massachusetts Institute of Technology. Project MAC involves research into the security aspects of large-scale virtual memory systems. A portion of this effort is devoted to the development of a secure kernel for the Honeywell Multics Computer. Support is jointly provided by the Advanced Research Projects Agency, the Air Force, and Honeywell.

One of the first credible commitments was the establishment by DOD of a Computer Security Evaluation Center at the National Security Agency in January 1981. "This center evaluates commercial computer systems and products, and publishes an evaluated products list that describes how secure a product is and the kind of environment in which it is suitable."[20] The National Security Agency has also created "Tiger Teams" which consist of government computer experts who secretly attempt to penetrate classified computer systems, having no more access than a trusted employee. This process helped define computer vulnerability.[21]

These are positive administrative steps at the national level, but the important step is at the user level. An operational security plan must be constructed at the ADP facility level. Some key questions are: who develops the ADP security plan; and is that person a physical security specialist, a communications security specialist, a computer systems analyst, or a computer programmer. DOD directs that the Automatic Data Processing System Security Officer is the person responsible for developing the security plan. DOD Directive 5200.28 stipulates that the ADPSSO is responsible for developing an ADP systems security program. That program covers all hardware and software functions and characteristics; operations procedures, accountability procedures, and access controls at the central computer facility and remote computer and terminal sites; management constraints and physical structures and devices; personnel; and communications control needed to provide an acceptable level of protection for classified material contained in the computer system.[22]

Usually, the newly appointed ADPSSO is a trained computer programmer, but is not trained in security. This lack of security training has caused an unacceptable void between security and computer operations. The new ADPSSO soon discovers that this part-time job is a full-time responsibility, and a headache. To carry out that responsibility the ADPSSO needs to develop a series of concentric zones of physical, contingency, personnel and technical security plans to protect the ADP facility's stored data. These buffer zones will serve as positive countermeasures to deter the hostile agent from finding critical paths of access into the system. The ADPSSO must identify possible paths of unauthorized access into each zone and emplace countermeasures that block physical or technical penetration. Concentric zones of security are:

Zone 1. Physical Security Zone: Intrusion, Penetration, and Deliberate Damage or Destruction. AR 380-380, Automated Systems Security, stipulates: "A balanced ADP security program must include a solid physical security foundation."[23] Physical security is the most important step in constructing the first line of defense against a hostile attack. Physical security should be designed into the facility during the planning phase of facility construction. A detailed environmental study is required to support the integration of physical security measures. The facility's power requirements, fire control procedures, air conditioning, and backup systems must be assessed. The ADPSSO will use the Department of Commerce's ***Guidelines for Automatic Data Processing Physical Security and Risk Management*** publication to structure physical security programs for ADP facilities.

Dr. Richard C. Clark, a recognized authority on terrorism, points out: "For terrorist action to destroy or deny temporarily the use of certain computers, computer expertise is not necessary . . . a bomb, a fire, the denial of electricity or telephone circuits, or even a hammer would be sufficient.[24] The ADP security manager must build sufficient physical barriers in depth (fences, lighting, alarms, gates, doors, cypher locks, guards, and badge control) and devise workable access control procedures to deter the determined agent from gaining access to critical areas such as computer rooms, data control areas, data file areas, and mechanical equipment rooms. The computer room is the heart of the ADP facility. It contains the central processing unit, input and output devices, and control hardware. The computer room should be given priority for the application of the toughest security policies and procedures. Remember, locks can be picked, fences can be climbed, tunnels can be built, and alarm systems can be neutralized by a determined intruder. Therefore, stringent access control procedures should be developed to limit access to the computer center. The room should be monitored by closed-circuit television cameras, have anti-intrusion alarms and a guarded entrance, and be checked periodically by roving security guards. Additional devices (photoelectric, infrared beams, and motion detectors) add protection that is extremely important during unoccupied hours. The security manager who posts signs stating: "This facility is protected by anti-intrusion alarms" has just alerted the intruder to potential obstacles that must be encountered and neutralized; security features should not be advertised. The ADPSSO should post concise, desk-side instructions on the proper action to take in case of bomb threats, fires, and power cutoffs. These procedures become useless if they are not practiced and tested on an announced schedule. A great deal of damage can occur from fires, but activated water sprinkler systems can

cause more damage than the fire itself. Water damages electrical circuitry, hardware, and data storage media. The HALON 1301 fire control system provides the best countermeasure to fire. It uses a chemical composition that smothers the fire but does not damage the hardware or software.[25]

Zone 2. Contingency Zone: Coping with Unforseen Damage or Destruction. Obviously, the ADPSSO cannot protect computer facilities from unexpected natural disasters (floods, earthquakes, tornados, or fires); however, he or she can develop contingency plans that offer alternate computer support if the main facility becomes non-operational. Contingency plans are necessary to minimize losses in cost, time, and efficiency of operations. DOD decision makers cannot afford a breakdown in computer operations during wartime emergencies.

While it may seem intuitively obvious that planning is imperative, it is often not practiced: In December 1981, the General Accounting Office published a report for Congress entitled "Most Federal Agencies Have Done Little Planning for Possible ADP Disasters."[26] The report describes how GAO inspected 55 federal ADP activities and discovered that none had an adequate ADP backup plan.

As a minimum, contingency plans must identify alternate ADP sites, file storage areas and backup software in case of emergencies. Any contingency plan must be tested to see if it works, and written plans must be tested to ensure that timely ADP support can be provided in emergencies.

The development of a workable contingency plan costs money, manpower and time to complete. However, since DOD has unwittingly created computer networks that require expensive backup facilities for each ADP site, contingency plans must be written to implement immediate actions required for emergency response, backup operations, and post-disaster recovery. In addition, DOD computer managers working in foreign countries should develop emergency destruction and removal plans that will be activated, if required, during wartime conditions. In all instances, contingency plans should be classified to protect them from unauthorized disclosure.

Zone 3. Personnel Zone: Personnel Security Protection. The ADPSSO must develop a security program that covers the protection of hardware, software, information, facilities, and personnel. People who have been granted security clearances are the most vulnerable targets in DOD. Clearances provide them access to the classified information desired by the hostile agent. It is well documented that espionage agents who have done the most harm to the security of the United States have held high-level security clearances. Therefore, the ADPSSO cannot rely totally on the government's background investigation program; rather, an individualized overwatch system has to be developed.

Most employees are granted Secret security clearances on the basis of a National Agency Check. This is simply a review of available records maintained by certain national agencies, including the FBI, to identify criminal behavior; it does not evaluate an individual's social, economic, or mental background. The ADPSSO, then, should be on the alert for indicators suggesting weaknesses in the character of employees, such as individuals who are deeply in debt, drinking heavily, taking narcotics or engaging in abnormal sexual behavior. Oliver R. Smoot of the Computer and Business Equipment Manufacturer's Association put it this way: "In the end, the human element is the ultimate weakness. The most effective way to break into a secure computer system is with a bribe, a pretty woman, or a handsome man to the right computer operator."[27] The overwatch system implemented by the ADPSSO must be used to identify and neutralize the vulnerable computer operator before the hostile agent does. This is a tough job in a society that cherishes individual privacy.

An effective personnel security program will ensure that all "personnel are aware of the special security needs of a computer center. Managers, system analysts, programmers, auditors, operators, and clerical personnel all have a part to play in computer security."[28] Personnel within the facility will require periodic security training which stresses their responsibility for document security, procedural security, communications security, and counterespionage.

Zone 4. Technical Zone: Hardware and Software Security. The technical zone of hardware and software countermeasures is the government's weakest security area. Lt. Gen. Lincoln Faurer, Director of the National Security Agency, states: "The threat to security ranges from the inadvertent dumping of material to a non-authorized recipient all the way to deliberate penetrations."[29] Therefore, the ADPSSO has to plan and develop security procedures which include methods of authenticating users, accounting for ADP disks and tapes, scheduling operations, and monitoring control systems.

In addition to procedures and plans, a total system security package for both hardware and software must be developed. This includes TEMPEST-tested communications equipment, encryption of classified traffic, password and audit trail systems to monitor access and use, and shielding to prevent hostile monitoring by electromagnetic devices.

The technical zone will be constructed by a computer systems analyst, a programmer, and data communications personnel. The security measures they develop must be protected, and only distributed to individuals on a strict "need to know" basis.

Before the ADPSSO can build the four concentric zones of computer security, he or she must initiate a continuing risk analysis program that will identify and evaluate critical paths of access that a hostile intruder could take to gain entry into each zone. A critical path is any physical or mechanical procedure used by an intruder to gain unauthorized entry into the system, be it the physical plant or the data.

A checklist or clipboard risk analysis is sufficient for initial guidance and identifying the environmental threat, but it will not determine the vulnerable, critical paths of hostile access. To be effective, the ADPSSO must reverse roles from defender to attacker and analyze the facility as would a hostile agent attempting to gain covert access. The ADPSSO must

"map out" the threat environment and determine what paths to take to gain unauthorized access. Since this is a difficult challenge for a non-trained counterintelligence agent to undertake, some help will be needed.

The ADPSSO should enlist the aid of a variety of experts—security specialists, counterintelligence agents, computer programmers, and systems engineers—to form a special team to identify and evaluate critical path vulnerabilities. This team would identify methods a hostile agent could use, and would actually conduct an attack to determine how far along the critical path one can travel before being detected. As the team uncovers vulnerabilities, it can construct additional security measures to correct the problem, thereby making each zone a solid ring of security.

Conclusions and Recommendations

The security of computer systems and related management problems are not new; in fact, they have been with us for some time. Why? Is it that resistance to innovations occurs because hardware and software security is too expensive to design, or that the cost-benefit ratio cannot be analyzed, or that senior DOD management is not fully advised of the problem? As intelligence managers, it is important to remember that there exists no method to determine how much classified information has been lost or compromised within our ADP facilities.

As long as this vulnerability in our national defense structure continues to exist, there will be potential problems in the realm of our national security. To counter this threat, the following actions should be initiated to enhance the level of security at DOD computer facilities:

- Creation by the services of new skill identifiers for computer security specialists and development of joint training programs that produce trained computer security and counterintelligence specialists to fill ADPSSO positions.
- Authorization of the ADPSSO position as a full-time duty position with a supporting staff that can manage the ADP security program.
- Resolution of commercial design problems and design of computer hardware and software security devices and programs that will preclude remote penetration and unauthorized browsing.
- A stronger contingency plan effort to mandate formal validation of annual testing.
- Extended background investigations on all personnel working in computer facilities.
- Service establishment of a dedicated research and development effort for service-peculiar security problems.
- Development of better methodologies for assessing potential threats to DOD computer facilities. ★

Footnotes

1. Klein, Melvin H., "Computer Security," ***Signal***, April 1983, pp. 11-19.

2. Department of Defense Computer Institute (DODCI), ***Selected Computer Articles 1980***, September 27, 1983.

3. Ibid., p. 207.

4. Mann, Sandra, "Tactical Planning for Data Security Management," DODCI ***Selected Computer Articles 1983-84***, *pp. 138-145.*

5. Babiak, Nick, Lt. Col., USAF, Personal Interview, September 6,1983.

6. United States Army Intelligence Agency (USAINTA), ***Computer Security Handbook*** 1976.

7. Ibid., p. III-2.

8. Bernhard, Robert, "Breaching Systems Security," ***Institute of Electrical, Electronics, Engineers Inc. Spectrum (IEEES)***, June 1982, pp. 24-31.

9. ***Computer Security Handbook 1976***, p. III-2.

10. Ibid., p. III-2.

11. Ibid., p. III-2.

12. Ibid., p. III-2.

13. Foster, Alfred, "Computer Security: Stopping the Super-Zappers," ***Government Computer News*** (June 1983), pp. 4-7.

14. Kelly, Orr, "Pentagon Computers: How Valuable to Spies," ***U.S. News and World Report***, October 31, 1983, pp. 36-37.

15. Ibid., p. 37.

16. ***Computer Security Handbook 1976***, p. III-3.

17. Volkman, Thomas L., "Computers—America's Achilles Heel?" ***Air University Review***, Vol. XXXIV, No. 4 (May-June 1983), pp. 43-47.

18. DODCI, ***Special Managing Automated Information Systems Resources Protection Course for Korea,*** August 6, 1982.

19. Ibid., pp. 20.

20. Peterson, Ivars, "Computer Crime: Insecurity in Numbers," ***Science News***, Vol. 122 (July 1982), pp. 12-14.

21. Kelly, pp. 36-37.

22. Department of Defense Directive 5200.28, ***Security Requirements for Automatic Data Processing Systems***, December 18, 1972, p. 2-2.

23. Department of the Army Regulation (AR) 380-380, ***Automated Systems Security***, October 14, 1977, p. 3-1.

24. Clark, Richard C., ***Technological Terrorism***, Devin-Adair Co., Old Greenwich, Conn., 1980, p. 149.

25. Guynes, Steve, "Software Security: Legal Aspects and Traditional Considerations," ***Journal of Management Systems Management***, Vol. 32, April 1981, pp. 34-38.

26. DODCI, ***Special Managing Automated Information Systems Resources Protection Course for Korea***, pp. 5-52.

27. Peterson, Ivars, p. 14.

28. Demis, Van Tassey, ***Computer Security Management***, New Jersey; Prentice-Hall, Inc., 1972, p. VII.

29. Kelly, p. 36.

Maj. N. Glenn Blackburn is currently serving as a strategic intelligence officer, Defense Intelligence Agency, Washington, D.C. He has a BA from the University of North Carolina and an MS from Southern Illinois University. He has served as the brigade intelligence officer for the 172nd Light Infantry Brigade (Separate). Other positions held are: infantry platoon leader, reconnaissance platoon leader, Special Forces commander, operations officer, counterintelligence agent, and tactical intelligence officer. Blackburn served with the 101st Airborne Division in Vietnam and has worked as an assistant professor of military science. He is a graduate of the Military Intelligence Advanced Course, Electronic Warfare Staff Officer Course, Special Forces Officer Course, Norwegian Language School, and the Armed Forces Staff College.

USAICS Notes

JINTACCS Update

The Joint Interoperability of Tactical Command and Control Systems message and data element standards are scheduled to be fully implemented by September 30, 1986. Certain combined and interservice interfaces will be added to the list when appropriate. To update Army intelligence and electronic warfare personnel, the following milestones were established in the U.S. Army JINTACCS Implementation Plan, October 1984 (final draft):

July 1985—Command and General Staff College begins teaching JINTACCS standards and procedures.

September 1, 1985—Major commands report to the Department of the Army the number of personnel to be trained and training materials needed.

October 1, 1985—Services, agencies, and unified commands receive initial training materials.

January 1, 1986—JINTACCS Standards receive joint approval.

January 15, 1986—Services, agencies, and unified commands receive users manuals.

February 1986—JINTACCS training/operational manuals disseminated.

March 1, 1986—JINTACCS training teams teach MACOM personnel; schools begin classroom training.

3rd Quarter FY 86—Modification of unit SOP and other documents to accommodate JINTACCS standards.

September 30, 1986—JINTACCS standards implemented across joint interfaces during field training exercises, command post exercises, and all joint operational data exchanges.

To be determined—JINTACCS standards implemented in software (automated systems) when available.

This implementation schedule is programmed with or without automated assistance. In response to a request for a computer assisted message preparation capability (CAMP), the Department of the Army emphasized currently programmed automated support to operational requirements and added that equipment to solely support CAMP will not be designed or purchased.

Army intelligence and electronic warfare personnel will ultimately use only one message and data element standard: JINTACCS. Many IEW systems/interfaces will be automated, and application of the JINTACCS standards will be implemented by fielding these automated systems/interfaces.

For more information on systems interoperability or standard issues, write to Commander, USAICS, ATTN: ATSI-CD-SI, Fort Huachuca, Ariz. 85613-7000, or call Mr. Barfield at Autovon 879-5825/3431. For training issue information, write ATTN: ATSI-TD-NSP, or call Mr. Alston at Autovon 879-3727.

Intelligence in Terrorism Counteraction Course Prospectus

The Intelligence in Terrorism Counteraction Course was developed by the U.S. Army Intelligence Center and School in 1984 based on the growing needs for trained terrorism intelligence analysts. The course was designed with the thought that an effective intelligence analyst must be thoroughly familiar with all aspects of terrorism, including terrorist tactics, strategies, goals, organizations, ideology, indicators, counteraction techniques and analytical procedures.

The main purpose of the ITC course is to provide military intelligence and other selected military and civilian personnel with a working knowledge of international, transnational and local forms of terrorist movements, trends, threats, targets and modus operandi. The subjects within the course are intelligence oriented, based on case studies with emphasis on intelligence operations, threat analysis and operations security assessments.

Because of the dynamic nature of terrorism, the program of instruction is flexible, thought provoking and designed to address the increasing terrorist threat to U.S. forces in the United States and overseas. Current terrorist situation and threat briefings are presented in each course.

The ITC Course is divided into three phases: The Terrorist Threat; Terrorist Strategies, Tactics and Indicators; and Terrorism Counteraction Intelligence.

Phase I, The Terrorist Threat, is subdivided into blocks on terrorism in a contemporary society; terrorists and their organizations; a primer on Marxist ideologies; new terror international; and the development and dynamics of international terrorism.

The subdivisions of Phase II, Terrorist Strategies, Tactics and Indicators, are anatomy of a terrorist incident; terrorism in action; major groups and organizations; terrorism in democratic society; terrorist weapons, bombs and explosives; terrorism in Latin America; and the kidnapping of Brig. Gen. Dozier—lessons learned.

Phase III, Terrorism Counteraction Intelligence, includes blocks on countering the terrorist threat; intelligence support of terrorism counteraction; terrorism analysis; legal aspects of terrorism and terrorism counteraction; hostage situations; and protection against terrorism.

The ITC Course number is 3C-F14/244-F8. Course length, for both peacetime and mobilization, is two weeks. The course is open to active Army, Army Reserve and Army National Guard personnel and selected Department of Defense civilians assigned or projected for assignment to terrorism counteraction duties. It is also for key intelligence personnel assigned to areas with high terrorist incident rates. The course requires a Secret clearance.

The ITC Course is also open to other services and government agencies; however, due to the length of the course, the emphasis is on Army intelligence doctrine, programs and operations from the U.S. Army Terrorism Counteraction Operational Concept (TRADOC Pam 525-34), and applicable Army regulations.

Quotas for military and civilian personnel are assigned by HQ, TRADOC, ATTG-MPS, Fort Monroe, Va. 23615 (Autovon 680-2161). Reserve and National Guard personnel must request attendance on DA Form 1058 through their unit to their respective headquarters.

Upon receipt of an attendance quota, students are required to submit their name, rank and SSN to TRADOC 45 days prior to the start of the course. One copy of orders must be sent to Commander, Co. F, 2nd School Battalion, 1st School Brigade, USAICS, Fort Huachuca, Ariz. 85613-7000, at least 30 days prior to the class date to allow sufficient time for billeting and administrative arrangements. Students should also contact the course manager a minimum of ten days prior to the class date. The course manager's address is Commandant, USAICS, ATTN: ATSI-HI-CI-LIC, Fort Huachuca, Ariz. 85613-7000. Telephone numbers are commercial area code (602) 538-5615/3453 or Autovon 879-5615/3453.

USAISD Notes

USAISD Instructor of the Year

Mr. Robert W. Caplin, an instructor in the Theory Branch, Electronic Maintenance Division, Maintenance Training Department was named the USAISD Instructor of the Year for 1984. Maj. Gen. Sidney T. Weinstein, commander of the U.S. Army Intelligence Center and School, presented the award to Caplin and the two runners-up February 21, 1985, at the Bull Run Restaurant in Shirley, Mass.

Caplin enlisted in the Army in 1954 and served as a radar repairman. His assignments included tours in the Philippines, Vietnam, and Berlin. After 20 years in the Army, Caplin retired in 1974. He began a second career in 1978 as an instructor at the Intelligence School, Fort Devens. A master instructor, Caplin was named Instructor of the Month for June 1980 and August 1984. He was first runner-up for Instructor of the Year in 1980.

For his accomplishment, Caplin was presented with an Army Certificate of Achievement, a nine-inch engraved silver bowl, and numerous prizes from local businesses.

Sgt. Stephan L. LeRoy, an instructor in the Basic Morse Division, was honored as first runner-up for Instructor of the Year. LeRoy was presented the Army Achievement Medal, a Certificate of Achievement, and other gifts from local merchants and associations.

Second runner-up was 1st Sgt. Chilton B. Shafer, first sergeant of Company A, 1st Battalion, 2nd School Brigade. Shafer, honored for his previous duties as an instructor in the Electronic Warfare/Cryptologic and Security Department, was also awarded the Army Achievement Medal, a Certificate of Achievement, and other prizes.

From left, 1st Sgt. Chilton B. Shafer and daughter Angela; Sgt. Stephen L. Leroy and wife Debra Keye; Mr. Robert W. Caplin and wife Mary; and Maj. Gen. Sidney T. Weinstein.

Officers Notes

Warrant Officer Training

After a two-year break, selected officer training has returned to the U.S. Army Intelligence School, Fort Devens.

Under the Army's new Warrant Officer Training System, all soldiers selected for an appointment to warrant officer will attend a six-week Warrant Officer Entry Course. Upon completion of the course, taught at Fort Rucker, Ala., Fort Sill, Okla., and Aberdeen Proving Ground, Md., the warrant officer candidates attend specific MOS training at their branch school.

Signal Intelligence/Electronic Warfare warrant officer candidates attend a five-week common core at Fort Huachuca before specific MOS training at Fort Devens.

USAISD currently conducts seven warrant officer courses, each offered six times per year. The MOSs taught are: Traffic Analysis Technician (MOS 982A), Emanation Analysis Technician (MOS 983A), Morse Intercept Technician (MOS 984A), Non-Morse Intercept Technician (MOS 985A), Emitter Location/Identification Technician (MOS 986A), Voice Intercept Technician (MOS 988A), and Electronic Warfare/Intercept Equipment Repair Technician (MOS 285A).

USAICS Update Line

The U.S. Army Intelligence Center and School has established an information update line that individuals may call for information on MOS changes, doctrine, class schedules and other areas of general interest. Information may be placed on the update line by writing to: Commander, USAICS, ATTN: ATSI-DA, Fort Huachuca, Ariz. 85613-7000. To call the update line, use Autovon 879-1782, or commercial (602) 538-1782.

The Junior Officer Cryptologic Career Program

by Capt. Donald J. Ball

The Junior Officer Cryptologic Career Program was established in 1971 by the Director, National Security Agency, to provide the military services with a select cadre of highly trained officers possessing an extensive background in signals intelligence. The program responded to a need to expose selected junior officers to the broad functions of the SIGINT effort, provide them with opportunities to learn and apply cryptologic skills, formally train them in the technical and managerial aspects of SIGINT, and allow them to see the relationship of the national SIGINT effort to the intelligence efforts of other agencies. JOCCP was established as a three-year tour at NSA, Fort Meade, Md., with an initial complement of 12 officers from three services. Currently, the Army, Navy and Air Force are each authorized ten participants in the program, while the Marine Corps is authorized four. Efforts are underway to increase the authorized number of Army participants to 15. To date, 120 officers have graduated from the program including over 40 from the Army.

Upon program entry, each officer begins a three-year tour consisting of varied and demanding operational assignments coupled with a rigorous academic curriculum in related technical fields. Each officer is required to complete a minimum of four six-month operational assignments during which the emphasis is placed upon being a productive, contributing member of the work force. Three of these assignments must be in the areas of traffic analysis and reporting, ELINT/EW, and collection management. Many participants complete a fifth tour in an area specifically related to their following assignments. In addition, each participant must complete 1,000 hours of academic course work in NSA's National Cryptologic School. Several courses are mandatory and include SIGINT analysis and reporting, computer science, traffic analysis, SIGINT technology, and the Military Cryptologic Officers Advanced Course (CY-500). Officers are also afforded the opportunity to attend courses offered by other intelligence agencies within the Washington, D.C. area.

The final product of JOCCP is an officer fully functional in the operations and management of both national and tactical level SIGINT efforts as a direct result of being technically qualified through both academic training and on-the-job experience.

(continued)

Follow-on assignments for Army JOCCP graduates may be with either tactical or strategic SIGINT units. It must be emphasized that the program does not just qualify individuals to serve as field station operations officers. An equal, if not greater need for qualified SIGINT officers exists in tactical units as well. With the arrival of a wide variety of new, technologically advanced tactical SIGINT assets in the Army inventory and the recognition of this increased emphasis by tactical commanders in combat electronic warfare and intelligence units, the potential contribution of a JOCCP graduate at this level becomes even greater.

Although the JOCCP is only in its fourteenth year, many of its graduates have already reached key positions in the SIGINT community where their training and experience are paying high dividends. Senior cryptologic officers from all the services enthusiastically endorse JOCCP as a direct result of the significant contributions graduates have made in their units. Although JOCCP allocations are limited, it is a program worthy of consideration for Army officers planning a career in SIGINT.

Criteria for application to JOCCP are: The applicant must be a SIGINT officer (SC 37) who has demonstrated outstanding performance and potential; the applicant must have a bachelor's degree, have not more than 12 years of service and be an O3; additionally, each officer must be an advanced course graduate and be eligible for a three-year assignment to Fort Meade. Although not mandatory, previous company command and tactical experience are beneficial to applicants.

Officers meeting the criteria must submit a written request for acceptance in the JOCCP to MI Branch at MILPERCEN. Letters of recommendation from senior officers and former commanders may be included as supporting documents.

Selection for JOCCP are made at least twice yearly and generally correspond with the graduation of officers currently in the program. There are no fixed dates for application or selection per se; specific information on projected openings may be obtained from MI Branch, MILPERCEN.

Enlisted Notes

97B10 Program Reinstated

The U.S. Army Intelligence Center and School has received approval from the U.S. Army Training and Doctrine Command to reinstate Military Occupational Specialty 97B10 (Counterintelligence Assistant) training. This approval was predicated on complete concurrence and strong support of the program from Soldier Support Center, National Capitol Region. The 97B10 program first started in May 1979, but due to several systemic problems, training was halted in August 1981. USAICS took action to correct previous problems and ensure that the revised program would be successfully implemented.

The importance of the 97B10 program to MI Branch and the Army cannot be overemphasized. The implementation of the Army of Excellence and new counterintelligence doctrine both demonstrate a need for junior 97B personnel; but perhaps most importantly, the 97B10 program will make the MOS sustainable and grade feasible. Current authorization documents and the resultant grade structure for MOS 97B require large numbers of senior non-commissioned officers, but few junior enlisted personnel. Staffed with branch transfers in the grades of E5, E6 and E7, the CI field is heavy with rank but light in CI experience.

The new 97B10 will be able to accomplish many tasks in support of CI missions at all echelons. The old program called for 97B10 personnel only at corps and below. The new 97B10 will accomplish more than typing, filing and motor maintenance. He or she will be trained in the latest CI doctrine based on the CI Operational Concept (TRADOC Pam 525-38, FM 34-60 and FM 34-60A). The result of this training will be a 97B10 capable of providing assistance in CI support to OPSEC, deception, the rear battle, and other CI missions. The key to success will be giving the 97B10 an opportunity to perform these activities.

97B10 training began in May. The 10-week, three-day course is taught at Fort Huachuca. After completing the course, the CI assistants are assigned to the field based on identified AOE positions. Until AOE is fully implemented, the USAICS Proponency Office will closely coordinate the assignments of 97B10 soldiers with MILPERCEN. A total of 225 positions have been identified for MOS 97B10: 140 at echelons above corps and 85 at echelons corps and below. The original intention of assigning one 97B10 to assist two or more senior agents has been maintained. During FY 85, 100 soldiers will be trained as CI assistants and another 100 are projected for FY 86.

The 97B10 program will progressively solve the shortage of MOS 97B. The MOS will become grade feasible and sustainable, and the quality and experience of 97B20 soldiers will be far greater.

For more information on the 97B10 program, contact the Department of Human Intelligence, USAICS, at Autovon 879-5551/5583.

10th Annual Army Intelligence Ball

The 10th Annual Army Intelligence Ball will be co-hosted by the Army Assistant Chief of Staff for Intelligence and the Commander, U.S. Army Intelligence and Security Command on Friday, September 27, 1985, at the Bolling Air Force Base Officers Club, in Washington, D.C. For more information, call the INSCOM Protocol Office at Autovon 222-5053.

Book Review Policy

Book reviews are considered to be an integral part of the presentation of information of professional interest to the MI community. The normal policy of ***Military Intelligence*** is to publish reviews of books which have appeared in print over the previous year. Book reviews which are more than one year old are only published in cases where useful subject matter might not otherwise have been brought to the attention of our readers. Such reviews are considered on a case-by-case basis. Reviews of current books are more likely to be published. A limited number of books are received directly from publishers and are available for review. If you are interested in reviewing one of these books, please contact the editorial staff. Unsolicited reviews are also welcome and encouraged.

"Feedback" is the readers' column, *your* column. Letters printed in "Feedback" can be on any subject that relates to intelligence, electronic warfare, doctrine, tactics, innovations from the field, suggestions, criticism, even praise, or anything else the readers of ***Military Intelligence*** may find of interest. Letters *do not* have to refer to a previously printed article or letter from the magazine to be used in

FEEDBACK.

Letter Policy: All letters to the editor must be signed. Names may be withheld if requested. Letters should be type-written and double spaced. The editor reserves the right to shorten letters. Letters are normally edited for style, grammar, spelling and punctuation. Please include a phone number (Autovon preferred) and a complete return address on the letter itself (envelopes tend to get separated from the letters).

Military Intelligence Writer's Guide

MILITARY INTELLIGENCE is oriented toward active Army, reserve and civilian intelligence personnel throughout the Army and Defense Intelligence communities. When writing an article, consider the readers. They range from privates to general officers to civilians, and they all have one thing in common: they work in, or have interest in, military intelligence.

SUBJECTS: We are interested in all subjects relating to the diverse fields of military intelligence including Army doctrine and policies relating to intelligence; tactical and strategic intelligence; organization; weapons and equipment; foreign forces; electronic warfare; and intelligence collection (SIGINT, HUMINT, IMINT, ect.). Historical articles should have contemporary value. If you have an idea for an article, contact us and explain your theme, scope and organization. It will save both of us time and will facilitate our planning.

STYLE: **Military Intelligence** prefers concise and direct wording in the active voice. Every article should have a beginning that catches the readers' attention, a body containing the crux of the article, and an ending which concludes or summarizes. Keep the article as simple as possible. Avoid unfamiliar terms, unexplained abbreviations, and poorly constructed sentences. Don't submit a manuscript unless you are completely satisfied with it. Read it over three or four times and then let a friend read it. It is not uncommon to revise an article several times before submitting a finished manuscript. Don't waste the readers' time with meaningless or repetitive phrases or words. We edit all articles. However, a polished article is more likely to be accepted than a hurried mistake-riddled effort. Save yourself time and effort; be your own editor. We do not normally allow writers to review how their articles have been edited.

ACCEPTANCE: We make no prior commitments on acceptance until we have thoroughly studied each manuscript. All manuscripts must be original, previously unpublished works. Authors submitting articles are responsible for informing the staff of **Military Intelligence** of simultaneous submission and/or acceptance by other publications.

FORMAT: We prefer articles from 1,000 to 2,500 words in length. We will publish shorter or longer articles depending on quality. Develop your ideas and stop. Send clean, doublespaced manuscripts typed on one side of the sheet. Your name, length of manuscript, address, and phone number (Autovon preferred) should be typed on the first page. We prefer one original and one copy. Cite your references and enclose all quoted material in quotation marks. If possible, credit should be given within the article as footnotes are burdensome and use valuable space.

GRAPHICS: Artwork in the form of black and white glossy photographs, maps, sketches or line drawings can enhance the attractiveness and effectiveness of your article. If you have an idea for artwork or know where we can get it, let us know.

CLEARANCE: All service members and Department of Defense civilians must clear articles through their local security office prior to submission. A signed statement of clearance must accompany the article. Certain categories of articles, as outlined in AR 360-5, must be cleared through the Office, Chief of Public Affairs, Department of the Army. Your local information officer can assist with this.

BIOGRAPHY: Enclose a brief biographical sketch, including important positions and assignments, experience or education which establishes your knowledge of the subject, and your current position and title. Photos of authors are no longer used in **Military Intelligence.**

COPYRIGHT: **Military Intelligence** is not copyrighted. Acceptance by **Military Intelligence** conveys the right for subsequent reproduction and use of published material for training purposes.

If you are interested in a subject, chances are that others will be too. Pick a subject, thoroughly research it, and think all your ideas through. Write with enthusiasm, but be natural. Don't adopt a different style.

For more information, contact the editor by writing to Commander, USAICS, ATTN: ATSI-TD-MIM, Fort Huachuca, Ariz. 85613-7000; or call Autovon 879-2676/3266, or commercial (602) 538-2676/3266.

Military Intelligence

Order Form

Mail To: Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

Enclosed is $ _____ ☐ check, ☐ money order, or charge to my Deposit Account No.

☐☐☐☐☐☐☐–☐

Order No._____

MasterCard and VISA accepted.

Credit Card Orders Only
Total charges $_____
Fill in the boxes below.
Credit Card No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Customer's Telephone No.'s
Area Code | Home | Area Code | Office

Expiration Date Month/Year ☐☐☐☐

Charge orders may be telephoned to the GPO order desk at (202)783-3238 from 8:00 a.m. to 4:00 p.m. eastern time, Monday-Friday (except holidays).

Please enter my subscription to MILITARY INTELLIGENCE *[MILIN] for one year at $14.00 Domestic; $17.50 Foreign.*

Company or Personal Name

Additional address/attention line

Street address

City State ZIP Code

(or Country)

PLEASE PRINT OR TYPE

For Office Use Only

Quantity	Charges
_____ Publications	
_____ Subscriptions	
Special Shipping Charges	
International Handling	
Special Charges	
OPNR	
_____ UPNS	
_____ Balance Due	
_____ Discount	
_____ Refund	

982

Military Intelligence

Order Form

Mail To: Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

Enclosed is $ _____ ☐ check, ☐ money order, or charge to my Deposit Account No.

☐☐☐☐☐☐☐–☐

Order No._____

MasterCard and VISA accepted.

Credit Card Orders Only
Total charges $_____
Fill in the boxes below.
Credit Card No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Customer's Telephone No.'s
Area Code | Home | Area Code | Office

Expiration Date Month/Year ☐☐☐☐

Charge orders may be telephoned to the GPO order desk at (202)783-3238 from 8:00 a.m. to 4:00 p.m. eastern time, Monday-Friday (except holidays).

Please enter my subscription to MILITARY INTELLIGENCE *[MILIN] for one year at $14.00 Domestic; $17.50 Foreign.*

Company or Personal Name

Additional address/attention line

Street address

City State ZIP Code

(or Country)

PLEASE PRINT OR TYPE

For Office Use Only

Quantity	Charges
_____ Publications	
_____ Subscriptions	
Special Shipping Charges	
International Handling	
Special Charges	
OPNR	
_____ UPNS	
_____ Balance Due	
_____ Discount	
_____ Refund	

982

MI Branch Notes

This is the first installment in a continuing series written by the assignment officers at Military Intelligence Branch, Military Personnel Center. Each future edition will attempt to examine and acquaint the reader with different areas of the assignment process or with recent updates in military personnel policy.

Branch Visits and Official Files

Currently, an appointment is not required to review branch files or to have an interview with an assignments officer. Interviews are taken on a first come, first served basis; however, MI Branch recommends individuals call the day before the visit to confirm that the appropriate branch representative will be present. A recent change to MILPERCEN policy establishes that official files (official microfiche and current ORB) will be reviewed through MI Branch. To obtain the microfiche and ORB in time for a scheduled visit, an appointment must be made at least 72 hours in advance. Appointments are made by calling the appropriate assignments officer. This appointment is necessary only to obtain personal copies of the official microfiche and ORB. Individuals unable to visit MILPERCEN may request copies of their official files by writing to MILPERCEN, ATTN: DAPC-MSR-R, 200 Stovall Street, Alexandria, Va. 22332-0400. There is currently no charge for these copies.

Officer Record Brief

Officers frequently question the duty title entries under Section IX (Assignment History). Duty titles used on the ORB should coincide with those used on the DA Form 67-8 (OER). This title does not have to be the same title as the MTOE slot the officer is assigned against, but should, rather, reflect what the officer is actually doing.

New Voluntary Indefinite Procedures

MILPERCEN has implemented a new voluntary indefinite centralized selection process for Reserve commissioned officers applying for voluntary indefinite extension on active duty. Officers who applied and were approved for Conditional Voluntary Indefinite status prior to December 1, 1984, are not subject to the provisions of the new selection process.

Reserve commissioned officers on the active duty list who have completed at least two years active federal commissioned service on their current tour, and who desire to remain on active duty beyond their initial obligation must apply for a CVI extension as specified in Interim Change 2, AR 135-215.

Officers must apply for CVI status between the twenty-fourth and twenty-seventh months of active federal commissioned service, regardless of initial active duty obligations. CVI applications, including a recommendation from the command, must arrive at MILPERCEN, ATTN: DAPC-OPF-P, not later than the twenty-seventh month of AFCS. Applications must include a statement that the officer understands that rebranching may be required to fill Army needs in exchange for continued active duty, to include listing three understrength branch preferences. If the officer wants to volunteer for an understrength branch, the request should be included in the application in addition to the three branch preferences. Volunteers for rebranching will be considered prior to the centralized selection board's decision on mandatory rebranching. Officers selected for rebranching will be rebranched upon promotion to captain or completion of their initial active duty service obligation, whichever comes first.

CVI applicants will be considered at least two months prior to completion of their third year of active duty. Officers selected for CVI status are granted an eight-year extension on active duty, unless sooner separated, released or retired from active duty in accordance with AR 635-100, AR 635-120, or AR 635-40. Officers incur a one-year active duty service obligation upon approval of their CVI extension. The service obligation, commensurate with the CVI extension, starts upon completion of the initial service obligation. In addition, an officer's extension of active duty may be revoked during the first year of the active duty service obligation for misconduct, moral or professional dereliction, or substandard performance of duty.

The centralized board will consider the officer's overall manner of performance, selecting only those officers judged best qualified based upon their performance and potential compared with all applicants of the same year group. In addition to selecting officers for extention of active duty, the board may reassign officers in excess of active duty needs to Reserve components upon completion of their obligated tour; release poor performers at the end of their obligated tour and recommend to the Army Reserve Components and Personnel Center that elimination action be initiated; or rebranch officers who are in excess of Army needs in certain branches.

Reserve officers serving in a CVI status who desire to remain on active duty upon completion of eight years AFCS must apply for final voluntary indefinite status between 81 and 87 months AFCS. Selection and rebranching criteria remain similar to the CVI process, with board consideration accomplished two calendar quarters before completion of the eighth year of AFCS.

Advanced Civil Schooling

Each year, MI Branch selects officers to attend advanced civil schooling under various programs. The Army provides these officers with an educational opportunity and assigns them to positions calling for that educational background periodically throughout their careers.

The Army has two general categories of programs: fully-funded and partially-funded. Under the fully-funded program the Army provides a permanent change of station move, full pay and allowances, tuition, and up to $200 per year for textbooks and supplies. Under the partially-funded program officers must pay for their own tuition, textbooks and supplies.

Officer quotas for the fully-funded program are determined by specialty codes and positions validated by the Army Educational Requirements Board. Quotas are no longer based on shortage disciplines. The current policy is that selectees must obtain a degree in an academic discipline which supports one or both of their specialties.

The majority of officers with advanced degrees will attend school by a PCS move or permissive TDY at no expense to the government. Applicants able to complete degree requirements in the least amount of time will be selected first.

Officers in fully-funded or degree completion programs at the graduate level must serve in a validated utilization position for three years to apply the education. Graduates who serve an initial utilization tour will be re-utilized on a periodic schedule, consistent with Army requirements and officer professional development needs.

Officers must meet the following prerequisites:

- Normally have no less than seven and no more than 13 years of commissioned service.
- Be fully qualified in the initial specialty at the tactical and nontactical levels.
- Have MI Officer Advanced Course credit (MEL 6).
- Possess a top-level military performance record.
- Have a good undergraduate degree record.
- Send a complete application with supporting documentation to MI Branch.
- Be available for a PCS move at the requested school start date.

Officers must apply for graduate school under the provisions of AR 621-1. Officers are selected by MI Branch through an informal board composed of branch members. Advanced civil schools boards are held as needed. Students participating in fully-funded programs are required to obtain a degree which supports one of their two specialties.

The following, although not all inclusive, is a list of academic disciplines which support MI Specialties:

35 (Military Intelligence)

- **Command, Control and Communications**
- **EW Systems Technology**
- **Area Studies**
- **International Relations**
- **Foreign Affairs**
- **Civil Government**
- **Geopolitics**
- **Political Science**

36 (CI/HUMINT/SIGSEC)

- **Foreign Language Literature**
- **Electronic Engineering**
- **Electrical Engineering**
- **Area Studies**
- **International Relations**
- **Foreign Affairs**
- **Civil Government**
- **Geopolitics**

37 (EW/Cryptology)

- **Command, Control and Communications**
- **EW Systems Technology**
- **Electrical Engineering**
- **ADPS Engineering**
- **Math Cryptanalysis**

For more information, contact Capt. Barbara Fast at MI Branch.

HOW TO CONTACT MI BRANCH

The mailing address for Military Intelligence Branch is:

U.S. Army MILPERCEN
ATTN: DAPC-OPF-M
200 Stovall Street
Alexandria, Va. 22332-0400

All official correspondence should be sent to this address. Use of specific attention lines to individual assignment officers is encouraged when mailing documents or requests. Whenever mailing a personnel action to MI Branch, telephonically notify the assignment officer of intentions.

The following points of contact and phone numbers were current as of June 1, 1985. MILPERCEN Autovon exchange is 221; commercial area code and exchange are (202) 325.

Chief, MI Branch	Lt. Col. James A. Bartlett	0143/0144/0145
Col. Assignments	Lt. Col. Edward D. Baisden	7877
Lt. Col. Assignments	Maj. James Murphy	0143/0144/0145
Maj. Assignments	Maj. G. Dickson Gribble	0143/0144/0145
Capt. Assignments	Maj. David Eggle	0143/0144/0145
Company Grade Assignments	Capt. John Custer	0143/0144/0145
Warrant Officer Assignments	CW3 Walter Johnson	7841/7842
Enlisted Assignments	Lt. Col. Byron Dean	0141
Professional Development	Capt. Barbara Fast	0143/0144/0145
Career Programs	Maj. Pat Gagan	8152/8153
Personnel Actions, CSAD, OPMF	Capt. Michael Lansing	7444

Officer Evaluation Reports

Active duty officers with questions relative to receipt of OERs at MILPERCEN or senior rater profiles pertinent to OERs in their files should call:

A-K 8667/8668 L-Z 8669/8670

MI Information Line

Military Intelligence Branch provides information on available assignments, professional development and other items of interest. A recording of this information is available on extension 7433.

Leadership Notes

Being a Mentor

by Capt. David A. Molten

When was the last time you stepped back from your busy routine and conducted a self-evaluation of your leadership style? If you are like the majority of our leaders, you probably feel that you just do not have the time for any self-evaluation. If that is true for you, check yourself while reading this article and see how your leadership style compares with the Army's leadership doctrine of *Be*, *Know*, and *Do*.

An excellent way to compare your leadership style to the doctrinal style is to determine whether or not you consider yourself to be a *mentor* to your subordinates. The leader who is a mentor is the type of leader who lives the Be, Know, Do doctrine everyday.

A mentor is a leader who understands that different motivational techniques need to be used because of the various ways in which his or her subordinates respond to motivation. A mentor is also a communicator who understands how to break down the many barriers which can inhibit communication between people, no matter how many. A mentor also realizes how important counseling is to the development of a cohesive unit. Using these skills of counseling, communication and motivation, a mentor creates the foundation upon which an effective team is built.

But what exactly is a mentor? By definition a mentor is a *trusted* counselor and guide who has the commitment of a guardian and the duty of a tutor. *A mentor has a personal stake in the positive development of his or her subordinates* because both mentor and charge share the same profession.

How does the mentor develop his or her subordinates in a positive manner? One way is to accept the role of being a teacher. As a teacher, the mentor provides goals and standards for his or her subordinates to achieve and surpass. When providing these goals and standards, the mentor is also providing a sense of direction toward where the unit is trying to go. To help subordinates achieve the goals and standards, the mentor establishes the motivational climate in which they operate. Some of the techniques that the mentor can use to develop subordinates are performance counseling, instructing and being a role model. Remember, these are just a few of the ways in which a teacher can assist in the development of his or her subordinates.

Another way in which a mentor can influence a subordinate's development is by becoming a coach. As a coach, the mentor teaches his or her subordinates how to accomplish a particular task by demonstrating the exact steps required for successful task accomplishment. After demonstrating the task, the mentor provides time for subordinates to practice the task, and gives immediate and precise feedback on task performance.

Combining the roles of teacher and coach, the mentor adds the final ingredient—the sincere concern that subordinates are improving as soldiers capable of handling the many missions in today's Army on the Air-Land Battlefield.

It is this personal ingredient that distinguishes the mentor from the teacher or the coach. The mentor is passing along knowledge gained through years of experience. Subordinates can improve on this knowledge as they become the leaders of the future.

Are you a mentor?

PROFESSIONAL READER

Red Flag Over Afghanistan: The Communist Coup, the Soviet Invasion, and the Consequences by Thomas T. Hammond, Boulder, Colo.: Westview Press, 261 pages, $11.95 paperback.

This book is revealing. It provides its readers with a historic perspective on how a nation becomes a Soviet satellite through no fault of its own. In the case of Afghanistan, its geographical proximity to Tsarist Russia and later to the Soviet Union made it fair game for Tsarist and Soviet imperialism. In fact, prior to the December 1979 Soviet invasion, there were three significant Soviet military and political efforts to bring Afghanistan into the Soviet sphere; these occurred in 1926, 1929, and 1930.

Afghanistan has never been a socially or politically united nation, but rather one separated along tribal and ethnic lines. Efforts by successive central governments to control the tribal clans were consistently unsuccessful. Prior to the emergence of the Afghan Communist Party as the dominant political power, the rulers of Afghanistan consisted of a succession of kings, first Amanullah, then Zahir. Each tried in his own way to maintain "cordial" relations with the Soviet Union. However, rule by the royal families was characterized by ineffectual and corrupt governments. It was, nevertheless, the even worse administration of President Daoud (1973-1979) that opened the door to the April 1978 communist coup.

Until the coup of 1978, the Afghan Communist Party had not made significant inroads into winning over the hearts and minds of the Afghan people. After the coup, a Democratic Republic of Afghanistan was proclaimed with President Taraki at its head. A short time later, Taraki's attempts to communize Afghanistan created intense dissatisfaction and caused revolts against his government. The situation in the Afghan countryside was so bad that the Soviet government felt it necessary to send a high level military/political delegation to Afghanistan to assess the internal situation. This same Soviet delegation reported back to Moscow that the internal security situation was worse than feared and that Taraki should be removed from office as quickly as possible. A coup was launched under Amin (Taraki's deputy) and Taraki was subsequently imprisoned and later executed. Amin's rule over Socialist Afghanistan (September-December 1979) faired as poorly as his predecessor's and the Afghan population intensified its resistance against the government in Kabul. It was against this backdrop that President Amin "invited" the Soviet army into Afghanistan in December 1979.

An invasion force numbering approximately 100,000 entered the country and Amin was taken into "custody" and was later executed along with the rest of his family. The Soviets brought in another prominent member of the Afghan Communist Party, Barbrak Karmal, the type of individual the Soviets could count on to do their bidding. Since the invasion, the Soviet army has destroyed many Afghan villages and cities. They have also launched military pacification campaigns that have resulted in many thousands killed and with many more millions forced to flee to Pakistan.

A good part of Hammond's book concerns the prospects of future Soviet rule in Afghanistan. Obviously the fighting will continue for many years. However, Hammond contends that without more Western aid in the form of military hardware, the Afghan resistance movement will eventually die. Hammond claims that "in the long run the most effective means for establishing Soviet control in Afghanistan is education and indoctrination. If it succeeds, the program will provide officers and soldiers for the army, bureaucrats, administrators, and spies for the infiltration of the rebels. To accomplish this goal, several thousand young Afghans are presently being educated in the Soviet Union and there are plans to send many more."

I highly recommend Hammond's book for those interested in the intense struggle being waged against the Soviet Union by the people of Afghanistan.

Michael S. Evancevich
U.S. Army, Retired

Fundamentals of Tactical Command and Control: A Soviet View by D. A. Ivanov, V. P. Seval'yev, and P. V. Shemanskiy. Translated and published by the U.S. Air Force; Soviet Military Thought Series 18. Washington: Government Printing Office, 333 pages, graphs and charts.

Published in Moscow in 1969 and translated for wide dissemination in the Warsaw Pact, **Fundamentals of Tactical Command and Control** examines Soviet C^2 concepts, systems, and decision making. Written for a knowledgeable reader, the book discusses command and control as the ultimate combat multiplier: the ultimate medium for synchronizing all available assets toward achieving the desired result. "Any control is carried out not for its own sake," the authors explain, "but so that the controlled object can achieve some purpose."

Opening with an historical and ideological overview of tactical command and control, the volume proceeds to C^2 organs, equipment, and control posts. The focus here is on how the system helps the commander attain an objective. Particularly interesting are the analyses of CP organization and restoration in combat.

The middle part of **Fundamentals of Command and Control** delves into war-gaming principles, statistics, and data systems. Readers will find these sections more informative than interesting, depending on the experience they bring to the subject. Step by step the authors trace the decision making process from staff estimates to analysis of the mission, from commander's concept to approval of a course of action, preparation of an order, and dissemination. The cycle is very similar to our own process for combat orders.

Final parts of the book touch on a number of areas—reconnaissance, security, camouflage, ECCM, rear services, weather, and terrain—that will have varying appeal to readers. The last three chapters, however, warrant careful reading by all serious students of the tactical and operational levels of AirLand war. These chapters deal with developing and maintaining troop morale, monitoring morale during the course of combat, and analyzing battlefield experience and disseminating this knowledge to the troops. Our military journals occasionally print articles on such subjects; but our military instruction and official publications lag far behind what the Soviets are doing in these areas.

Two points impress the reader. One is the high level at which this book is written. Our Soviet counterparts are well-versed in military doctrine, art, and science. Second, the book assumes that the effective military leader understands the political and philosophical foundations of command and control. Reading this volume teaches not only tactical fundamentals, but also gives a Soviet perspective on the close relationship between the fighting force and its ideological heritage.

Capt. Glen E. Lich
USACGSC

High Frontier: A Strategy for National Survival, by Lt. Gen. Daniel O. Graham (Retired),TOR Books, 1983, 314 pages, $7.95.

Lt. Gen. Daniel Graham, former Deputy Director, CIA, is eminently qualified to head a project with **High Frontier's** strategic ramifications. His experience is evident in the thorough research and sound conclusions upon which this "strategy for national survival" is based.

Graham proposes that the United States can and must quickly field a non-nuclear Global Ballistic Missile Defense using existing technology at a *net* cost of virtually nothing. **High Frontier** is one system—with variations—that fulfills that requirement.

Graham asserts that the U.S. strategic defense policy of Mutually Assured Destruction is not a defense policy at all. Since the purpose of a Soviet preemptive strike would be to destroy our means to retaliate, the best defense would instead be to prevent its success. A GBMD which makes the outcome of a Soviet ICBM assault unpredictable as to both how many and, more importantly, which U.S. missile silos and strategic assets will survive attack "changes the simple arithmetic problem (of eliminating U.S. weaponry into a complex calculus full of uncertainties, *and such uncertainties are the essence of deterrence*." (p.76)

Wishing to defend the United States rather than destroy the Soviet homeland, Graham assembled a research team including physicists, technologists, economists and other analysts to end-run the frightfully conservative thinking of the U.S. military and technologically end-run the Soviets as well. The team had no prior commitment to any agency.

The system proposed is startling and inspirational. The first phase would, within three years, field a point missile defense system; several are discussed. The Tracor SWARMJET is a mass multiple rocket launcher with a simple, survivable radar control. The GAU-8 30mm cannon would also be cheap and flexible. Either could destroy up to 90 percent of incoming warheads and cost less than silo superhardening.

Within six years, the next defense layer would use cislunar space—the new high ground—to base more than 400 intercommunicating orbital

"trucks" carrying projectiles that would destroy ballistic missiles immediately after launch. The "trucks" do not require precise orbits, but any vehicle sent to kill one would. This makes defeat of the system prohibitively expensive; the system itself would cost less than the MX. The "truck's" beauty is that it provides the United States with alternatives to preemptive strike, launch-on-warning, or retaliation. Said one spokesman, "We'd like to think that nothing we propose can be used to kill a Soviet schoolgirl." It *can* be used to destroy ballistic missiles with such confidence that they would probably not be launched. It can also defend itself—and other space assets—and be used as a basis for effective, survivable communications. Direct attack of the system would itself become an early warning of Soviet intentions.

Within a decade the final defense layer would probably incorporate beam weaponry to destroy those mid-trajectory ICBMs which escape boost-phase defenses. Concurrently, supporting systems including a spaceplane (service and maintenance), low-cost cargo boosters, solar power generation satellites, manned space stations, and civil defense systems must be developed. Total cost, without deducting predictable economic benefits, would be $30-50 billion.

Graham's cost estimates, developmental schedules, and system comparisons are comprehensively tabulated. He points out that even $100 billion would be a low premium for insurance of the *trillions* of dollars of defense and civil assets protected; there are fewer technological unknowns in all of **High Frontier** than in the 1950s when ATLAS was conceived. ATLAS was fielded within four years.

An adequate review of **High Frontier's** bold initiative would require a book in itself. The challenges to the system considered and successfully defended in his text are elegant. A technology which, if acquired by the Soviets as well, could only serve to prevent the possibility of global thermonuclear war deserves the undivided attention of the nation.

Capt. Jennifer R. Kumaran
Fort Huachuca, Ariz.

Nuclear Strategy and Strategic Planning by Colin S. Gray, Philadelphia: Foreign Research Institute, 1984, 130 pages.

This little volume, part of the Philadelphia Planning Papers Series, is a clearly written, even-handed condensation of almost 30 years of U.S. nuclear policy making. This book is not polemic. It gives the reader more than an exposition of the history of nuclear strategy. Dr. Colin Gray presents to the reader several alternate and radically opposing views and treats each fairly and openly. None of these views are presented as "straw man" examples; each is examined closely and in detail.

Gray, president of the National Research Institute for Public Policy, is qualified to serve as the author of this book. He has worked on the faculties of several universities in the United States and the United Kingdom and has authored many books and articles dealing with strategic nuclear policy and U.S. military policy. He has also served as Director of National Security Studies at the Hudson Institute and as Assistant Director of the International Institute of Strategic Studies in London.

One area that Gray explores is the mainstream of current nuclear strategic thought in the United States. He properly identifies this thinking as a policy of deterrence based on strong elements of counterforce, control and damage limitation. He adds that there is an evolutionary tendency towards a method of limiting damage through some sort of homemade defense (e.g. an active ABM system). He strongly believes that the American people support a policy of this nature contrary to what popular media suggest.

Another area that he explores in some detail is the current argument forwarded by some critics of U.S. nuclear policy that our Command, Control and Communications network is too vulnerable to nuclear attack and that it would not survive intact to produce an effective counterstrike. He claims that this is a tautological argument; the mission of a Soviet first strike would be to destroy our C^3 ability. For deterrence to be effective, as he suggests, there is an imperative that the United States modernize and improve its C^3 system and continue to concentrate on a policy of limitation and control of nuclear forces with an ability for controlled, graduated response.

This book is highly recommended reading for those in the military community who are interested in finding answers to the never ending debate on nuclear strategy. This work is eminently scholarly and includes a copious bibliography and a list of suggested readings.

1st Lt. John M. Lovett
Protocol Office
Fort Leavenworth, Kan.

Regionalism and Global Security by Gavin Boyd, Lexington Mass.: Lexington Books, 1984, 196 pages.

In a world increasingly seen as divided by two superpowers, we tend to either neglect or forget other countries' interests. To see the world as either American or Soviet is to lack comprehension and distort an understanding of current events. The European Common Market formed by Western European countries and the Organization of Petroleum Exporting Countries formed by Middle Eastern countries are two examples of regional focus that preclude superpower interests. Recognizing the potential for influence in today's world arena, regionalism has spread under the axion "united we stand, divided we fall."

Gavin Boyd, in his new book **Regionalism and Global Security**, suggests that it would be in the interest of the United States to further build and promote regionalism. Global security is not found in the development and proliferation of technologically advanced weaponry with higher kill rates, but through the promotion of new forms of international collaboration. "The building of the Third World regional communities (which include Africa and Latin America), a Pacific community, and a more active Atlantic partnership with deepening European integration would represent major advances toward world order." Boyd states the United Nations has been a failure due to factional self-interest among the individual countries; a possible remedy to this problem would be "restructuring of the U.N. system to cope with outstanding problems of representation and decision making on the basis of participation by regional structures rather than individual states."

The process of regional community building, under the guidance of the U.S., will necessitate vigorous and innovative statecraft. The U.S. must take the lead role due to its prominence and vast resources in providing the leadership for collective security and economic interdependence among the different regions of the world. For example, by supporting Third World regionalism, the developmental problems that require comprehensive regional economic cooperation can become more self-evident in the different world communities; thus vital imperatives can be undertaken for more self-reliant industrialization to foster regional commerce, reduce foreign corporate control and "acquire bargaining strength for negotiations with the major industrialized democracies on international trade and monetary questions."

In return for U.S. efforts to enhance intergovernmental interactions and market integration, a strong role would be guaranteed for the various regions of the world. Increased cooperation by the individual countries can only lead to collective security by forming a network of alliances that would shut out any Soviet efforts for global hegemony. In addition, the influence of the United States in world affairs has been weakening because of strains in its network of alliances and declines in its share of international economic activity; hence its need for cooperation from allies and trading partners has been increasing.

However, Boyd is not quixotic enough to overlook the disparity of economic, social, and political issues that plague regionalism.

Problems of regionalism in African, Latin American and Pacific community building are complicated by U.S.-Soviet confrontations. Furthermore, "the involvement of external power reduces the capabilities of individual leaders to respond to their problems in accord with their own sociocultural patterns." For example, while African leaders are uneasy about the presence of East European and Cuban advisors in Angola and Mozambique, they are even more concerned about the exploitations of this situation by the West that could engulf Africa in a U.S.-U.S.S.R. conflict.

This book begins to fill a void in international diplomacy that has been overlooked for too long. Regional community building, under the guidance and with the support of the United States, can inflict more caution on Soviet world design than a missile could ever have. While overcoming major handicaps, a strong effort must be made to enhance global security through regionalism by enhancing and remembering other than superpower interest.

Sp5 Jan Goldman
193rd MI Company
Panama

SYMBOLISM

Oriental blue and gray (silver) are the branch colors of Military Intelligence. The red dragon represents the Orient and the lineage of the 501st MI Group. The lightning bolt signifies worldwide electrical communication and the key symbolizes security and control; crossed in saltire, they represent strength and symbolize ASA and MI united. The swords are adapted from the MI branch insignia. Their colors, white and black, signify day and night and the continuous mission of the group.

501st Military Intelligence Group

Constituted on October 13, 1950, in the Regular Army as Headquarters and Headquarters Company, 501st Communication Reconnaissance Group, the unit was activated on October 20, 1950, at Camp Pickett, Va., and assigned to the Army Security Agency. On May 29, 1951, the 501st transferred from Camp Pickett to Camp Stoneman, Calif., for staging to Pusan, Korea.

The 501st arrived at Pusan on June 25, 1951. The unit spent the next four days in the Pusan assembly area tent city awaiting sea transportation to Inchon. The 501st arrived at Inchon Bay on July 1, and travelled by motor convoy to Seoul where a temporary headquarters was established in a two-story brick residential home located at Ka Hea Dong, Seoul. On July 13, the group headquarters moved into the war-damaged main building of the Kyanggi Middle School, Seoul. By July 15, 1951, the 501st had assumed administrative and operational control of all ASA units in Korea.

The 501st Communication Reconnaissance Group represented a first of its kind and a milestone in intelligence support to U.S. tactical troops. The Korean War presented ASA with the opportunity to test its newly formed doctrine in support of a Field Army. ASA activated the 501st Communication Reconnaissance Group to direct operations of ASA support units in the Korean Theater, coordinating all ASA activities at each of the low echelons.

By the end of hostilities in July 1953, the group had three battalions and five companies assigned. Actual strength of officers and enlisted men totaled more than 1,600. Besides the numerous citations awarded its subordinate units, Headquarters and Headquarters Company, 501st Communication Reconnaissance Group received the Meritorious Unit Commendation (July !, 1951 to July 27, 1953) and the Republic of Korea Presidential Unit Citation (July 15, 1951 to April 30, 1953) and credit for participation in six campaigns.

On January 28, 1956, the 501st Communication Reconnaissance Group was redesignated as Headquarters and Headquarters Company, 501st Army Security Agency Group. On July 1, 1956, the 501st ASA Group was inactivated and its personnel and mission transferred to the concurrently organized 508th USASA Group, a TDA organization, as part of worldwide reorganization occurring within the ASA to provide greater flexibility in support to tactical units.

On January 1, 1978, the Headquarters and Headquarters Company, 501st ASA Group was redesignated the Headquarters and Headquarters Company, 501st Military Intelligence Group and activated at Yongsan, Korea. The group took the place of the temporary 501st MI Group (Provisional), organized at Camp Coiner on April 1, 1977, as part of the major reorganization within Army intelligence which merged individual disciplines into one organization. Subordinate to the U.S. Army Intelligence and Security Command, the 501st MI Group exercises administrative control over INSCOM units in Korea and provides intelligence and security support to Headquarters, Eighth U.S. Army throughout Korea.

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

Penalty for Private Use $300

ISSN 0026-4028

Postage and Fees Paid
Department of the Army
DOD 314

Second Class Postage